総合演習－２
S-2. インシデント対応コスト

文京学院大学　浜　正樹
中部大学　岡部　仁

公益社団法人　私立大学情報教育協会

情報セキュリティインシデント情報と対応

- 組織内利用者からの情報・相談

- 組織外利用者からの情報提供、通報、捜査
  - 情報提供：　個人、組織（情報部門担当者等）
  - 通報：　IPA, JPCERT/CC等情報セキュリティ対応・監視組織
  - 捜査：　警察等

- その他

責任にある回答

対応組織（グループ）の現状

- CSIRT/SOCの存在？
- 活動実績？
- 自組織のみで対応が可能か？
  - **すべてをアウトソーシングできない！**
- 人材の確保と教育（時間的問題と経験）
- 情報の信頼性（専門家による第三者担保）
- その他

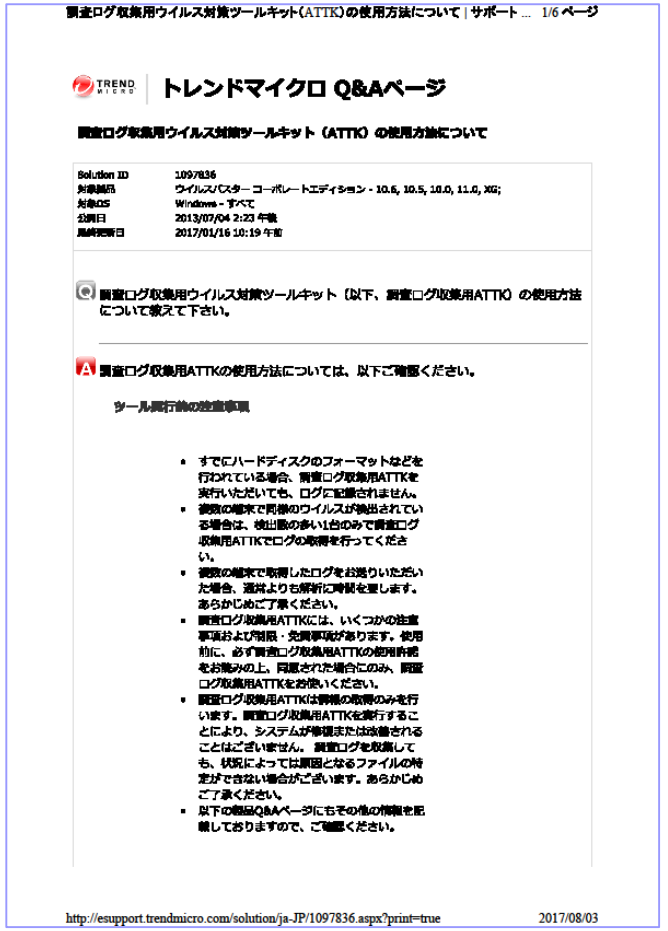
大学情報部門が情報セキュリティの最先端の専門家とあるべきか？

インシデント発生時

- **インシデントは事実であり、どのような情報と数（正確な）の把握**
- 初動対応の判断（インシデントに対し何が重要か？対応の優先順位）
- １１９番の準備ができているのか？
  - 火報は鳴る
  - 初期消火は、天井に火が届くまで等
  - 初期対応では手に負えない、および火災の原因究明（専門家）
- 火災防火訓練の実施（法的）

事前の準備と予算

- インシデント対応が、自組織のみで短時間で適切な情報収集ができるか？
- CSIRT等経営層に責任ある情報の提示
- できない場合の対応のため事前に業者を確保
  - 秘密保持契約を含む、事前の準備（準契約）
  - データ解析の内容（報告）と期間の確認（協議）
  - データ保全の手順書（1クリック）：　対応者
- 手配：　発生時に対応する契約（臨時予算の確保）
- 経営層への答申



調査ログ収集用ウイルス対策ツールキット(ATTK)の使用方法について | サポート ... 1/6 ページ

TREND MICRO トレンドマイクロ Q&Aページ

調査ログ収集用ウイルス対策ツールキット（ATTK）の使用方法について

Solution ID	1097836
対象製品	ウイルスバスター コーポレートエディション - 10.6, 10.5, 10.0, 11.0, XG;
対象OS	Windows - すべて
公開日	2013/07/04 2:23 午後
最終更新日	2017/01/16 10:19 午前

Q 調査ログ収集用ウイルス対策ツールキット（以下、調査ログ収集用ATTK）の使用方法について教えて下さい。

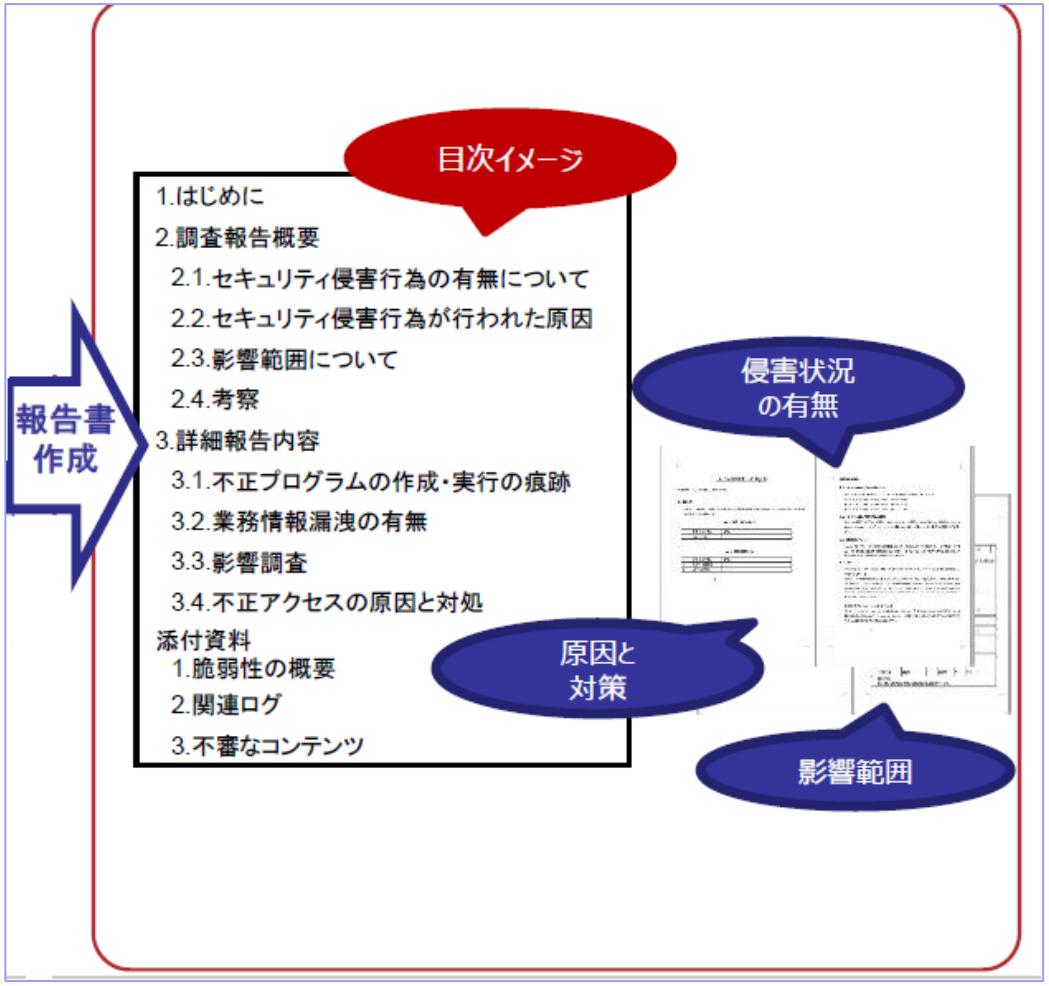
A 調査ログ収集用ATTKの使用方法については、以下ご確認ください。

ツール実行時の注意事項

- すでにハードディスクのフォーマットなどを行われている場合、調査ログ収集用ATTKを実行いただいても、ログに記録されません。
- 複数の端末で同様のウイルスが検出されている場合は、検出数の多い1台のみで調査ログ収集用ATTKでログの取得を行ってください。
- 複数の端末で取得したログをお送りいただいた場合、通常よりも解析に時間を要します。あらかじめご了承ください。
- 調査ログ収集用ATTKには、いくつかの注意事項および制限・免責事項があります。使用前に、必ず調査ログ収集用ATTKの使用許諾をお読みの上、同意された場合にのみ、調査ログ収集用ATTKをお使いください。
- 調査ログ収集用ATTKは情報の取得のみを行います。調査ログ収集用ATTKを実行することにより、システムが修復または改善されることはございません。 調査ログを収集しても、状況によっては原因となるファイルの特定ができない場合がございます。あらかじめご了承ください。
- 以下の製品Q&Aページにもその他の情報を記載しておりますので、ご確認ください。

http://esupport.trendmicro.com/solution/ja-JP/1097836.aspx?print=true 2017/08/03

業者サービスの一例



パンフレット

FUJITSU

FUJITSU Security Solution
セキュリティ侵害調査サービス

サイバー攻撃の被害状況を正確に把握

サービス概要

本サービスは、お客様から送付していただいた情報（HDDイメージ、ログ等）を詳細に調査・分析するサービスです。

セキュリティ侵害調査の特徴と効果

◆特長1：富士通のセキュリティエキスパートが、ハードディスクイメージ、各機器のファイル、ログ等の情報から、段階的に攻撃プロセスを特定しサイバー攻撃の特定を行います。
◆特長2：お客様から追加のログ提供があれば、各情報の因果関係を見つけ出しながら、サイバー攻撃の特定を行います。

効果

被害状況の明確化
攻撃者の不正活動の経過を把握することで、侵害状況の有無、原因、影響範囲が明確となります。

再発防止策の立案
被害状況から、被害発生に至る状況を正確に把握し、その後の対応方針について、短期的な暫定対処から、中期的な再発防止策を立案することができます。

サービスご提供イメージ

※オプションでお客様に対面での報告会を実施いたします。

shaping tomorrow with you