NTT AT

インターネット環境セキュアソリューション
デジタルフォレンジックサービス

情報セキュリティインシデントが発生！
記憶媒体から“隠された真実”を明らかにします。

最新のデジタル鑑識技術で、不正アクセスや標的型攻撃などの原因・被害内容を解析

デジタルフォレンジックサービス

“デジタルフォレンジック”とは、情報通信分野における不正アクセスや機密情報漏洩などのサイバーセキュリティインシデントにおける原因究明手段として、PCやサーバーなどの記録媒体やネットワーク機器のログファイルなどを分析し、その証拠を見つけ出す技術的作業の一般的な総称であり、本来は警察捜査の「法医学」や「科学捜査」、「鑑識」といった意味である“Forensics”から引用され、使われるようになった用語です。
NTT-ATのデジタルフォレンジックサービスは、不正アクセスに使われた遠隔操作マルウェアの発見・解析・除去や、脆弱性を狙った情報流出に関するネットワークのログ情報解析などで、その原因や流出した情報の詳細を特定するデジタル鑑識技術です。
経験豊富な専門技術者が高度な解析機器を駆使し、そこに“隠された真実”を明らかにします。


厳重な入退室セキュリティ完備の
解析専用ラボにおける解析風景

POINT 1
NTTグループで培った豊富な経験と実績

NTTグループ内においてセキュリティ関連業務に携わってきた経験豊富、かつ高度な知識を持った専門技術者が、お客様の課題にお応えします。

POINT 2
専用機器による高度な解析

専用機器（デュプリケータやフォレンジックソフトウェア）を用いた、正確な保全と入念な解析を行い、記録媒体やログに隠された真実を明らかにします。

POINT 3
高い機密性を備えた解析専用ラボ完備

極めて機密レベルが高い情報を取扱うため、解析専用ラボへの入室は生体認証により認可された解析担当者のみに制限しています。

■ インシデント発生事例とデジタルフォレンジック解析作業の一例

● 標的型攻撃によるインシデント発生

メール添付されたマルウェアを社員が誤って実行。ネットワークログを解析し、不正通信は特定できたが、マルウェアを含む二次検体の存在やその内容、感染端末で行われた操作、漏洩したファイルがわからない。

● 解析作業例

- マルウェア添付メールの復元/解析
- マルウェアの解析
- 外部通信痕跡の解析
- レジストリの解析
- VSSからのファイル復元
- 不審ファイルの実行痕跡とファイル解析
- 削除された漏洩ファイルのカービング

● 脆弱性を突いた攻撃による情報漏洩

認証を要求するWebサーバに不正コードを用いて脆弱性を突く攻撃が検知された。ネットワークログを解析し、どこまでのアカウントが被害にあっているのか、そのほかにどんな影響があるのかわからない。

● 解析作業例

- アップデート状況の確認
- コマンド実行履歴の確認
- 通信・認証ログの確認
- 設定変更内容の確認
- バックドアの設置の確認
- 不審ファイルの実行痕跡/ファイル内容解析
- 未割当領域を含む検索
- 漏洩ファイルのカービング

■ 主なサービスフロー

- 機密性の高い情報を扱うため、作業開始前にNDA（秘密保持契約）を締結
- お客様ご指定の場所での保全作業
  - ・お客様先での作業の場合、専用機器を持ち込みます。
- 弊社関係者のみが立ち入り可能なフォレンジックラボで解析作業を実施
  - ・解析作業期間は、通常1～2週間です。
  - ・調査依頼内容に応じて御社内のネットワークログ解析などもおこなう場合があります。
- 解析完了後に解析結果を報告書にまとめ、ご報告
- 調査完了後は、全作業データを消去、破棄

※詳細な仕様は、ご依頼内容や調査範囲により異なりますので、詳しくはお問い合わせください。

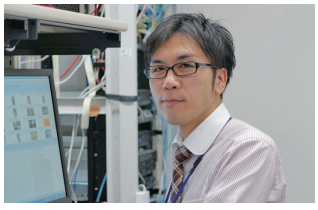
■ 価格

100万円～（解析の内容・規模・状況・対応体制・ご支援の範囲によって異なるため、詳細はお問い合わせください。）

デジタルフォレンジックは、豊富な経験と実績のあるプロにお任せください!

昨今、国内の企業や政府機関などを標的とし、世間を騒がせた最も大きなインシデントとして挙げられるのが、日本年金機構の情報流出事件です。これは通称「CloudyOmega（クラウディオメガ）」と呼ばれる攻撃活動において、遠隔操作マルウェア「Emdivi（エンディビ）」によって用意周到におこなわれ、約125万件という膨大な数の個人情報が流出しました。このような攻撃は、その手法や技術も日々進化し続けていますが、対して被攻撃側の対策が一向に追いついていないため、次にいつ、誰がターゲットになるか分かりません。
万が一、被害が発生してしまった場合、その全容解明と再発防止が何よりも重要ですが、ここで必須となるのがデジタルフォレンジック技術です。私たちは、これまで多くのサイバーセキュリティインシデントに対応した経験の中で、特にデジタルフォレンジックに関して数多くのノウハウがあり、全容解明と再発防止に向けて、確かな技術でお客様を全面的にご支援します。

NTTグループ内のサイバーセキュリティインシデント対策を担ってきたエキスパート



NTTアドバンステクノロジ株式会社
越谷 淳平

201604C

お問い合わせ先
TEL: 0120-318-311 E-mail: cyber-sos@ml.ntt-at.co.jp
http://www.ntt-at.co.jp/product/forensic/
NTTアドバンステクノロジ株式会社
トータルソリューション事業本部 デジタルフォレンジックサービス担当
〒212-0014 神奈川県川崎市幸区大宮町1310 ミューザ川崎セントラルタワー