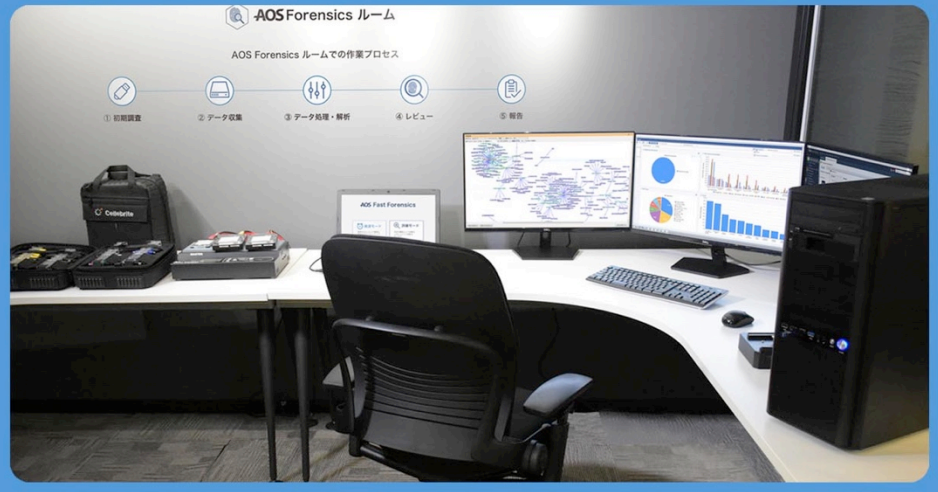
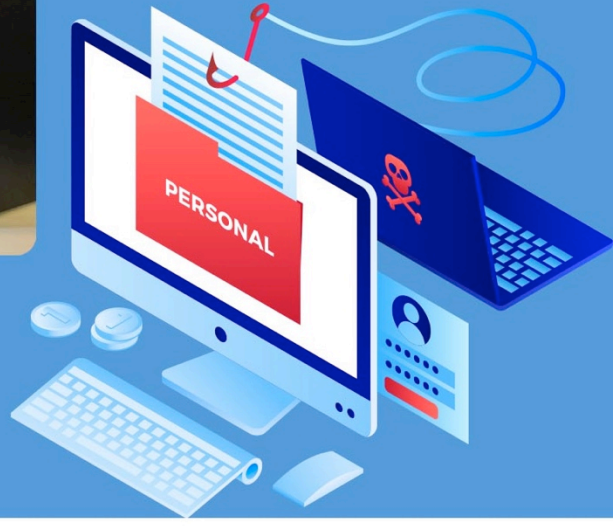


RegTech コンプライアンス・第三者委員会
～ 企業が自力でサイバー攻撃調査を行うために ～



RegTech インハウス・フォレンジック調査ソリューション

AOS Forensics ルーム サイバー攻撃 調査事例

リーガルテック株式会社
an AOS company

AOS Forensics ルームとサイバー攻撃

サイバー攻撃が多発しており、この対策を官民あげて強化することが求められています。サイバー攻撃に対応する有効な手段としてデジタルフォレンジックが注目されています。デジタルフォレンジック調査を行うと、ハッカーが消してしまったログを復元して、侵入の痕跡を調査したり、内部からの不正アクセスも効率良く調査することができるようになります。

インハウス・フォレンジックソリューション

「AOS Forensicsルーム」は、企業内において、サイバー攻撃の痕跡調査を行うことを目的として、企業内に設置されるフォレンジック調査官が作業を行うための専用ルームです。リーガルテック社は、AOS Forensicsルームの設立のためのコンサルティングからフォレンジックツールの選定、使い方のトレーニングを提供し、より高度なフォレンジック調査サービスを通じて、インハウス・フォレンジックルームの設置を支援いたします。

インハウス・フォレンジックの6つのメリット

・社内に適用すれば数億円を節約する戦略的なセキュリティ対策

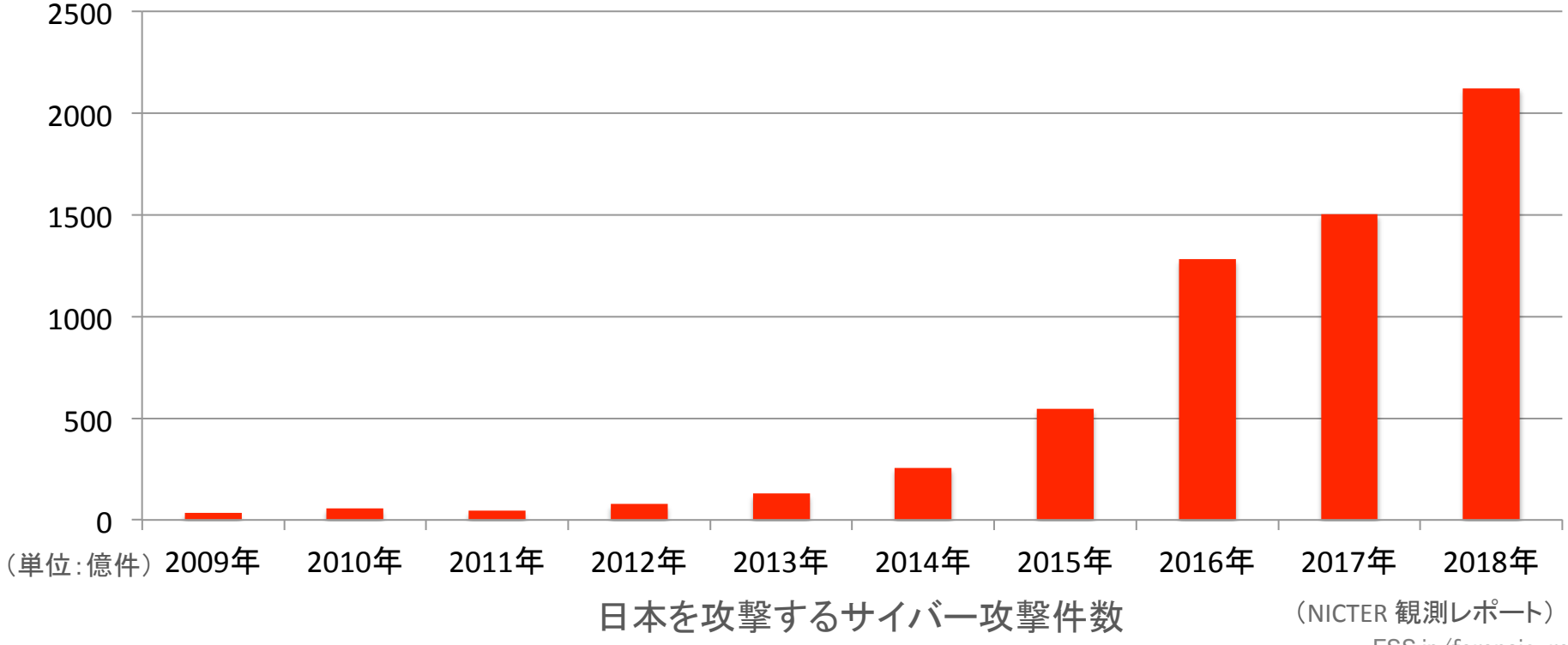
米国では38%の企業がセキュリティ戦略の一形態として
フォレンジックツールと手法を利用しています。

FSS.jp/forensic-room/

日本を攻撃するサイバー攻撃は、年々増加

日本を攻撃するサイバー攻撃は、2018年には、2，000億件を突破！

NICTERの観測レポートによると、日本を攻撃するサイバー攻撃は年々増加しており、2018年は、2,121億件となりました。



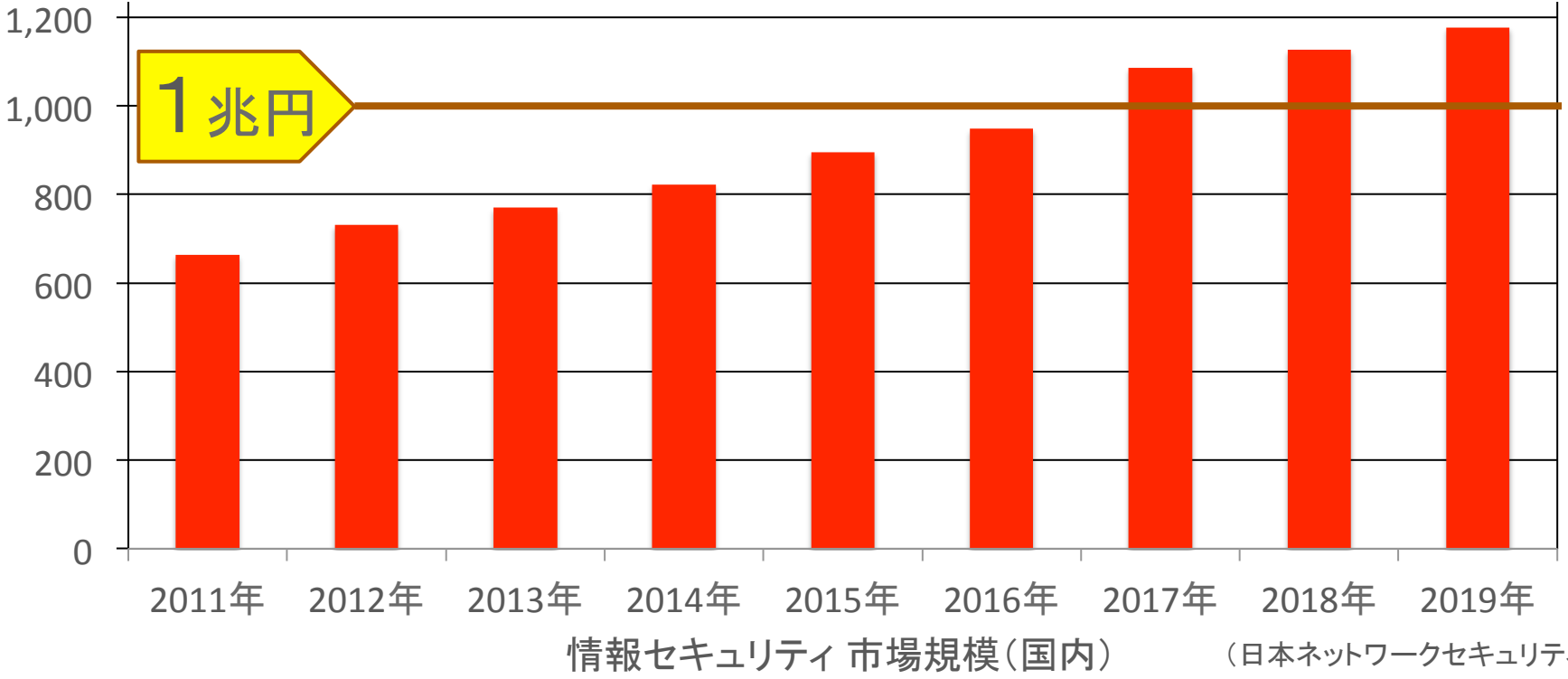
日本を攻撃するサイバー攻撃件数

（NICTER 観測レポート）

情報セキュリティ市場は、年々増加

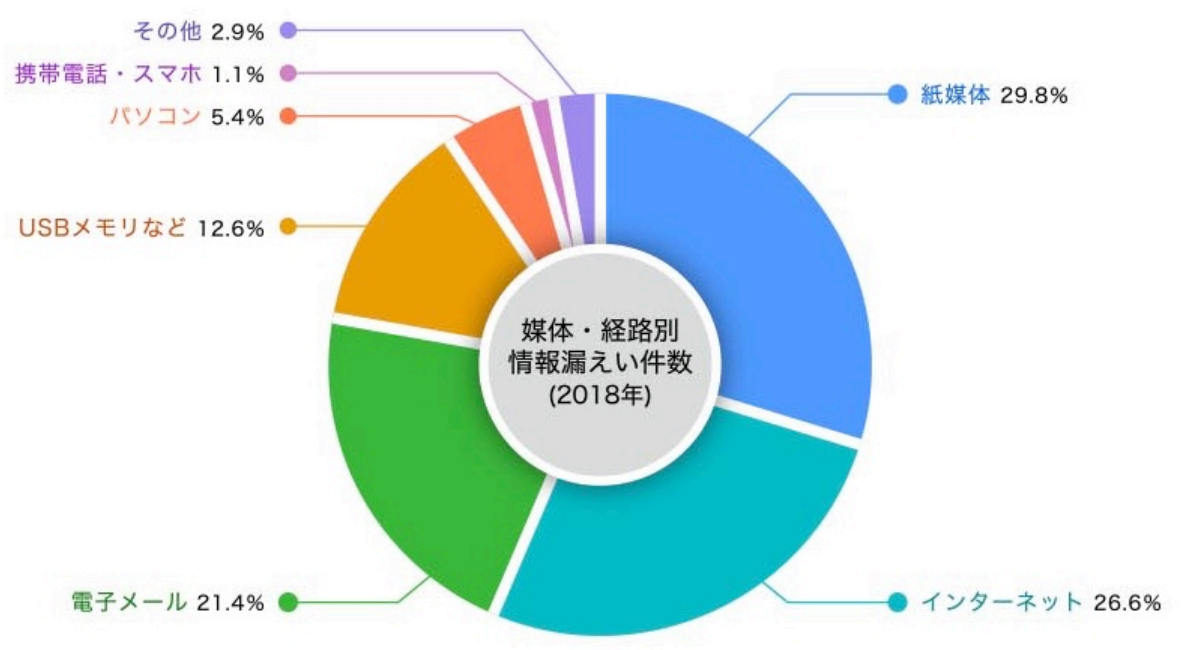
国内のセキュリティ市場は、2017年以降は、1兆円を突破！

日本ネットワークセキュリティ協会によると、国内の情報セキュリティの市場規模は、年々拡大しており、2017年以降は、1兆円を突破しています。



不正アクセスによる被害が増加

情報漏えいの原因を見てみると、近年は、不正アクセスによる漏えいが急増しており、サイバーセキュリティの強化が求められています。2018年の情報漏えいの媒体・経路別の比率を調べてみると、紙媒体からの漏えいが29.8%と一番多いのですが、紙媒体の比率は、年々減少しており、インターネット、電子メール経由の漏えいが増えています。インターネット経由は26.6%、電子メール経由は、21.4%、USB等の媒体経由が12.6%となっています。



媒体・経路別情報漏えい件数（２０１８年）

（日本ネットワークセキュリティ協会）

国内外のサイバー攻撃の事例

海外のサイバー攻撃の事例

世界最大のホテルチェーンマリオットで3億8,300万人の個人情報が流出
米マリオットは、宿泊客の予約データベースに不正アクセスがあったと発表した。約3億8,300万人の情報には、名前、住所、電話番号、メールアドレス、パスポート番号、カード番号などが含まれているとのこと。

－ 2018年11月30日

米司法省が中国軍ハッカー部隊を訴追
米司法省は、米企業へのサイバー攻撃に関与したとして中国人民解放軍の当局者５人を刑事訴追したと発表した。この攻撃を受けた東芝傘下の米原子力大手のウエスチングハウスは、４基の原子炉を中国で建設中だった１０年に、原子炉の配管などの設計情報を盗まれたとのこと。

－ 2014年5月19日

ソニー・ピクチャーズがハッキング攻撃を受け情報が流出
金正恩暗殺を描いたコメディ映画を非難していた北朝鮮のハッカーに攻撃を受け、関係者間での電子メール、従業員の個人情報、未公開の映画本編のコピーといった様々な情報が流出した。

－ 2014年11月24日

国内のサイバー攻撃の事例

ホンダの狭山工場のネットワークにWanaCryが侵入したことが発覚、工場が操業停止に至った。WanaCryは、日本、北米、欧州、中国など複数の地域の工場に侵入されたが、操業停止は、狭山工場のみだった。

－ 2017年6月18日

日本年金機構が不正アクセスを受け、１２５万件の個人情報が流出
年金管理システムがサイバー攻撃を受け、職員が電子メールに添付されたウイルスの入ったファイルを開封し、１２５万件の個人情報が流出した。

－ 2015年5月8日

日本国内の大手半導体メーカーでUSBメモリを経由して、品質検査を行う検査装置がマルウェアに感染した。感染により、検査プロセス処理の負荷が異常に高まり、本来不良品として判定すべきものがそのまま検出されずに通ってしまうという不具合が発生した。さらに感染元が分からず、感染が飛び火し、最終的には生産ラインが停止した。

－ 2011年

AOS Forensics ルームの活用メリット

企業がサイバー攻撃の対策として、AOS Forensics ルームを活用するメリットとして、予防法務としてのメリット、早期発見のメリット、事後対策としてのメリットの3つがあります。

予防法務としてのメリット

サイバー攻撃に対してのAOS Forensics ルームを導入することによる予防法務のメリットは、オプションのクラウドバックアップを導入しておくことで、ランサムウェアに感染した場合の被害を食い止める効果を発揮することです。

早期発見のメリット

サイバー攻撃の兆候が検出された場合に、専用のフォレンジック調査室があり、早期発見の能力を高めていることには、早期発見の精度を高め、損額を最小限に食い止めるという大きなメリットがあります。

事後対策のメリット

サイバー攻撃を受けたことが判明した場合には、迅速な対応が求められます。社内にフォレンジック調査室を備えておくことで、削除されたログを復元した解析することができ、事後対応を迅速に、しかもローコストで行えるというメリットがあります。

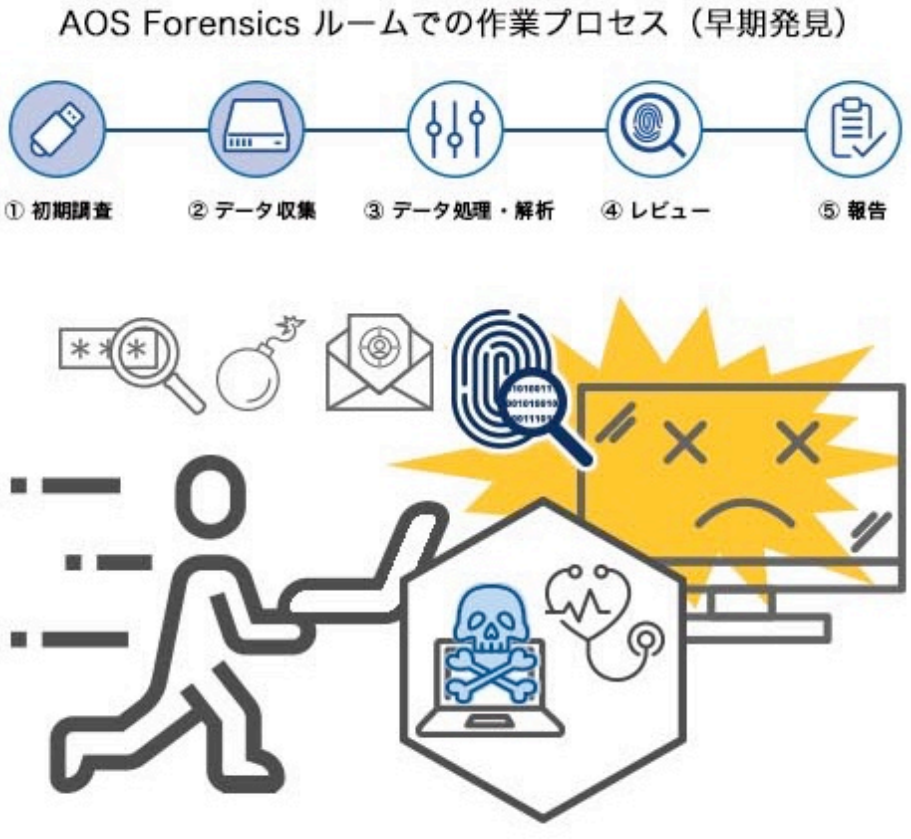
AOS Forensics ルームの活用メリット

予防法務としてのメリット

迅速の予防調査を社内で行える

AOS Forensics ルームを導入することにより、企業は、迅速に不正アクセス調査を社内で行えるようになります。
不正アクセスを調べるためには、データの改ざんの有無や消されてしまったログの調査が必要となりますが、これらの調査を行うためには、専門家がフォレンジックツールを使って調査を行う必要があります。
インハウス・フォレンジックとして、AOS Forensics ルームを導入すれば、外部の専門家に依頼しないでも、企業が社内でフォレンジック調査を行うことができるようになり、迅速に対応が可能となります。
また、事前にオプションのランサムディフェンダーやクラウドバックアップを導入しておけば、ランサムウェアの予防対策にもなります。

AOS Forensics ルームの活用メリット

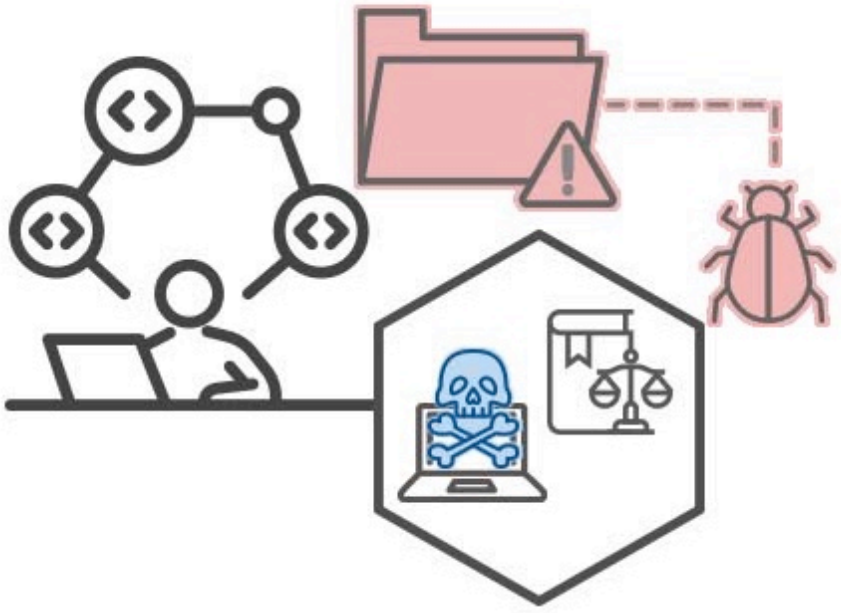


早期発見のメリット

不正の通報窓口を設置、内部通報制度の設立

サイバー攻撃の痕跡を早期に発見できれば、サイバー攻撃の原因を早期に調べることができます。
サイバー攻撃は、多発しており、サイバー攻撃の痕跡を早期発見できる能力を企業が備えることには、多くのメリットがあります。
サイバー攻撃を受けると、企業は甚大な被害を被りますが、早期に原因究明の能力を高めておくことで、迅速な対応が可能となります。
サイバー攻撃を行うハッカーは侵入の痕跡を削除するケースが多く、高度な復元調査能力を備えておくことで、早期の侵入経路の特定に有効な手段となります。

AOS Forensics ルームの活用メリット



事後対策としてのメリット

社内のデジタル証拠の調査で迅速に対応

サイバー攻撃を受けたことが判明し、事後対策が求められるなかで、自力でデジタルデータの証拠調査能力を備えておくことに大きなメリットがあります。
サイバー攻撃の兆候が検知された場合に、社内にフォレンジック調査室を設けていないと、十分なデジタル証拠の調査が行えず、侵入の痕跡を見つけることができずに、原因究明が遅れることにも繋がります。
社内でデジタル証拠の調査が行えれば、このような事態に迅速に対応することが可能となります。
また、オプションのクラウドバックアップを導入していれば、ランサムウェアの攻撃を受けて暗号化されてしまったデータを元どおりに戻すこともできます。

フォレンジック調査のプロセス

フォレンジック調査は、初期調査、データ収集（保全）、データ処理・解析、レビュー、報告の5つのプロセスで行います。初期調査では、調査対象となる機器を特定し、保全対象の優先順位を決定します。そして、調査対象となった機器の証拠性を損なわないようにコピーを行います。収集したデータをフォレンジックツールで処理し、復元、検索、分類などの解析作業を行います。処理されたデータをレビューし、証拠データを特定して、報告するという流れとなります。

初期調査

ファストフォレンジック調査により、調査開始時に調査の対象にしようとしている機器のデータの状態を速やかに把握し、保全対象と優先順位を決定します。

データ収集（保全）

調査対象機器内の証拠性を損なわないように、データの収集を行います。削除されたデータの復元が必要になる場合は、ディスクイメージの収集が必要となります。

データ処理・解析

収集したデータの解析、復元、検索、分類等を行います。優れたツールを駆使することにより、証拠調査能力を高め、迅速な分析ができるようになります。

レビュー

証拠を特定します。場合に応じて、レビュープラットフォームを使用します。最新のツールを駆使すれば、レビュー時間を大幅に削減することができます。

報告

報告書及び、報告用の最終成果物をまとめます。ケースに応じた報告書のフォーマットを活用することで、包括的な報告書を効率よく作成できます。

AOS Forensics ルームの提供内容

AOS Forensicsルームは、フォレンジック調査ソフトやハードウェアをコンポーネントで構成されたシステムとして提供し、調査室の設置、システムの使い方、フォレンジック調査の方法、調査官の教育及び研修、調査支援などを行いインハウス・フォレンジック調査室の構築を支援します。

- フォレンジックルーム設置支援
  - ルーム運用規定の策定支援
  - フォレンジック調査用ハード/ソフトウェアの選定と調達
  - 作業環境の構築支援

- フォレンジックトレーニング
  - 管理者向け・・・インシデント発生時の対応について
  - 技術者向け・・・各種フォレンジックツールの使用方法について
  - レビュー管理者向け・・・レビューの進め方やタグ、ステージについて

- コンサルティング
  フォレンジックの専門家がコンサルタントとしてフォレンジックルームに関する質問にお答えいたします。

リーガルテック社のサイバー攻撃の調査実績

政府機関のシステムに対し外部から「標的型攻撃メール」が送られ、その結果サーバーに保管されていた100万件を超える個人情報が漏洩した。
直接の原因としては、漏洩は職員宛てに送られた標的型攻撃メールにより起こった。

フリーアドレスから送られたこのメールは、「○○制度見直しについて（試案）に関する意見」等の件名で送信されており、開封や添付ファイルのダウンロードを行う事で、端末がウィルスに感染してしまった。

このサイバー攻撃は、国内の別のサーバーを踏み台として行われ、遠隔操作で情報を抜き取るように指示が出されました。

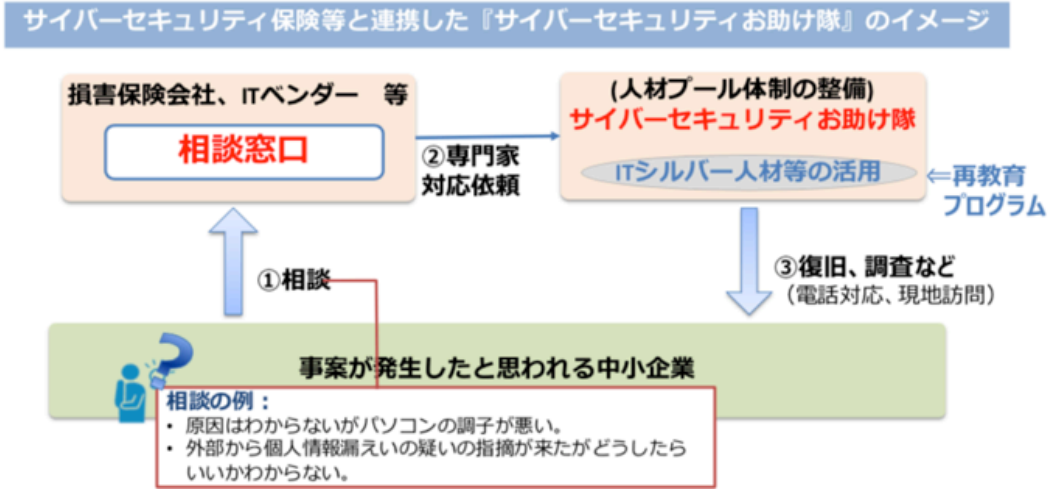
リーガルテック社は、踏み台とされたサーバーのサイバー攻撃の痕跡を調査するためにアクセスログの復元調査などを行い、外部からの侵入の証拠調査を行いました。

サイバーお助け隊にリーガルテック社のツールが採用

経済産業省は、サイバー攻撃から地域の中小企業を見守る「サイバーセキュリティお助け隊」の実証を始めました。宮城や広島、愛知など15府県で今夏から随時取り組みを始めています。
愛知県では、MS&ADインターリスク総研が実証事業を実施し、協力者として、ALSOKなどが参加しますが、ALSOKをサポートするソリューションとしてリーガルテック社が提供するAOS Fast Forensicsが採用されることが決定しました。

・サイバーセキュリティお助け隊の仕組み

サイバー被害を受けた企業から相談を受け付ける窓口を設置し、必要に応じて「サイバーセキュリティお助け隊」が出動し、問題解決にあたるという流れとなりますが、愛知県の実証事業では、ALSOKがこの「サイバーセキュリティお助け隊」を担当します。お助け隊のメンバーはITについての専門性が求められますが、ここで、AOS Fast Forensicsを活用することで、効率良く調査が行えるかを検証する実証実験がスタートしました。



法務のデジタルトランスフォーメーションをご支援いたします

リーガルテック株式会社 会社概要

設立 : 2012年6月

資本金 : 51,000,000円

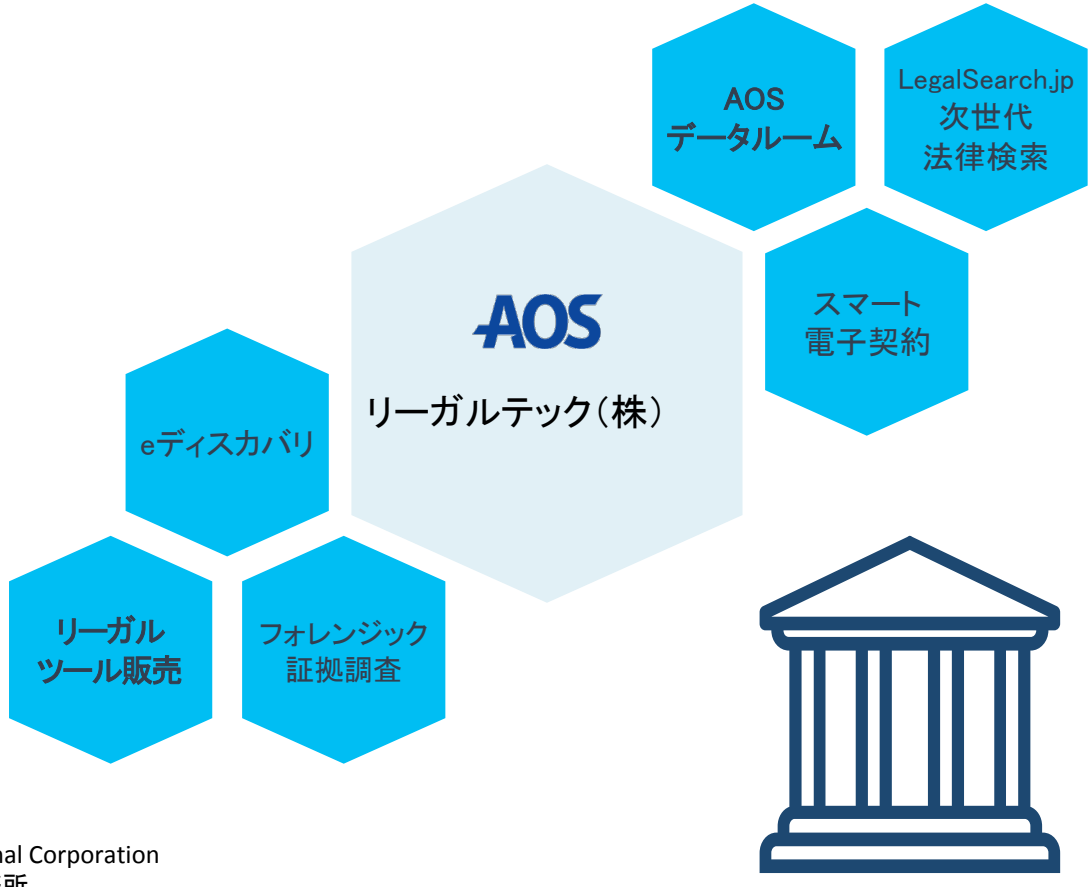
代表取締役 : 佐々木 隆仁

株主 : AOSテクノロジーズ（株）100%

事業内容 : VDR事業
eディスカバリ事業
フォレンジック事業
司法インフラ事業
（法律検索 LegalSearch.jp）

Web : AOS.com
LegalTech.co.jp

顧問弁護士 :
吉峯　耕平　田辺総合法律事務所
大井　哲也　TMI総合法律事務所
金井　高志　フランテック法律事務所
高橋　喜一　コスモポリタン法律事務所
清水　陽平　法律事務所アルシエン
大平　恵美　DSA Legal Solutions, Professional Corporation
赤坂屋 潤　表参道パートナーズ法律事務所
渥美　雅之　三浦法律事務所
高田　佳匡　鎧橋総合法律事務所



AOS Forensics ルーム

リーガルテック株式会社

〒105-0001　東京都港区虎ノ門5-13-1 虎ノ門40MTビル 4F
TEL：03-5733-5790　FAX：03-5733-7012

カンパニー長　古川 宏治　k.furukawa@aos.com
リーガルコンシェルジュ 笹野 由季子　y.sasano@aos.com

AOS.com
LegalTech.co.jp