RegTech コンプライアンス・第三者委員会
～ 企業が自力で情報漏えい調査を行うために ～

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 情報漏えい 調査事例

リーガルテック株式会社
an AOS company

AOS Forensics ルームと情報漏えい

個人情報漏えいのニュースがたくさん流れています。個人情報の漏えいは、どのような企業や個人でも起こる可能性がありますが、企業が引き起こす情報漏えいは、その企業に非常に大きなダメージを与えますので、何らかの対策が必要となります。情報漏えい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、情報漏えいの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/

情報漏えいによる想定損害賠償金額は、7兆円

個人情報漏えい人数は、累計で18億人を突破！

日本ネットワークセキュリティ協会によると、2018年に発生した個人情報漏えい件数は、433件で漏えい人数は、561万人、想定損害賠償総額は、2，684億円とのことです。
過去14年間では、累計18億5，236万人分の個人情報が漏えいしており、想定損害賠償金額の総額は、7兆2，106億円となります。

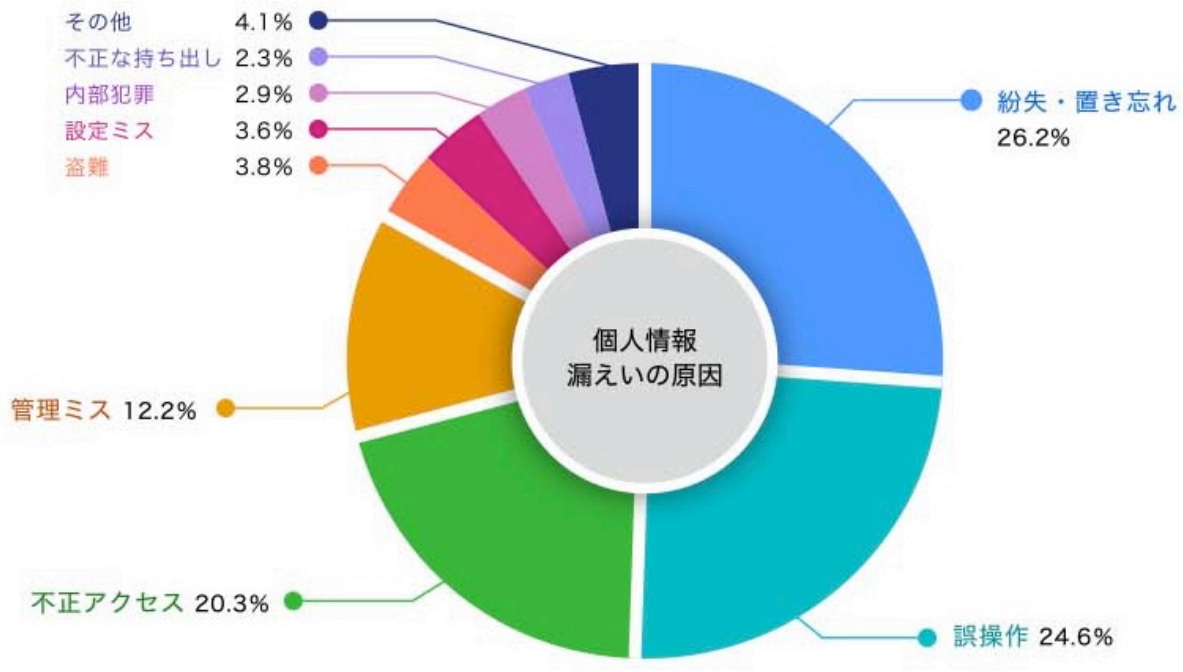
個人情報漏えい事件

	2018年	過去14年間累計
漏えい人数	561万3,797人	18億5,236万人
漏えい件数	443件	1万6,446件
想定損害賠償総額	2,684億円	7兆2,106億円

（日本ネットワークセキュリティ協会）

個人情報の漏えいの原因は、不正アクセスが増加

個人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、セキュリティの強化が求められています。
2018年の情報漏えいの原因を調べてみると、紛失・置き忘れが26.2%、誤操作が24.6%、不正アクセスが20.3%となっています。



個人情報漏えい原因（２０１８年）

（日本ネットワークセキュリティ協会）

国内外の個人情報漏えい事件

海外の個人情報漏えい事件

Facebookの４億1900万人以上の情報漏洩が発生

Facebook ID、電話番号、名前、性別、居住国などが管理者不明のデータベースでパスワードが設定されずにオンラインで公開されていた。。

－ 2019年9月5日

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

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

国内の個人情報漏えい事件

セブン・ペイで約900人分の個人情報が流出

セブン・ペイのサービス開始から３日後に漏洩が報道さえた。流出したのは、個人情報９００名分で、同時にアカウントに関連付けられたクレジットカード、デビットカードが不正に利用され、約5,500万円が不正使用される被害が発生し、セブンペイは、支払いサービスを廃止すると発表した。

－ 2019年7月3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

進研ゼミなどを運営する通信教育最大手企業であるベネッセコーポレーションで個人情報流出事件が発生し、最大3,504万人分の個人情報が流出した。

－ 2014年7月9日

AOS Forensics ルームの活用メリット

企業が個人情報漏えい対策として、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

個人情報漏えいに対しての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、会社が情報漏えいの痕跡を調べるフォレンジックルームを設置したことをアピールすることで、従業員による不正アクセスを抑止するという効果を発揮することです。

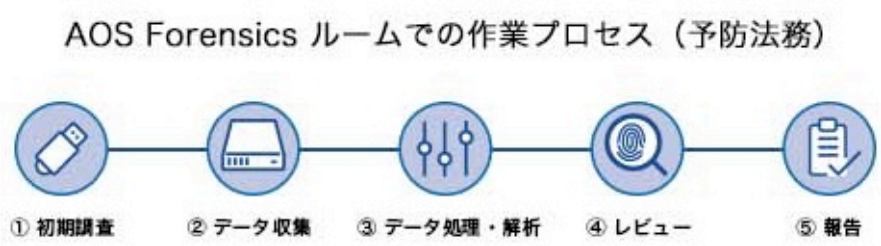
早期発見のメリット

個人情報漏えいの痕跡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、USBメモリの接続履歴調査や、ファイルの削除などを復元調査できることで、早期発見の能力を高め、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

個人情報の漏えい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、情報漏えいのルート調査のために削除されたログを復元解析するなどということが自社でできるようになり、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、迅速に個人情報漏えい調査を社内で行えるようになります。
個人情報漏えいを調べるためには、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、USBの接続履歴の調査などの社内調査を企業が自力で行えるようになり、迅速な漏えい調査が可能となります。また、オプションで個人情報を検出するプライバシーディフェンダーを導入すれば、個人情報を保護することができます。

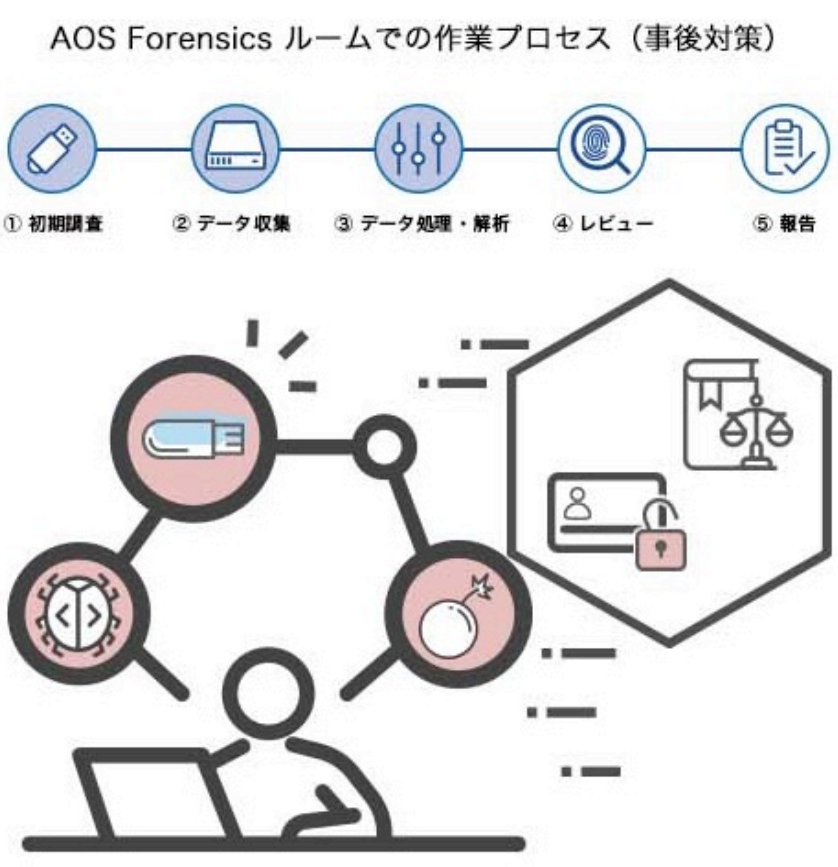
AOS Forensics ルームの活用メリット

早期発見のメリット

削除されたログの復元、USBメモリの接続履歴調査

個人情報漏えいの痕跡を早期に発見できれば、流出の原因を早期に調べることができます。
個人情報の流出は多発しており、個人情報漏えい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。
個人情報の流出事件が起こると、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。
個人情報の流出を狙う攻撃者は、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。
社内の個人情報を保管しているサーバーにアクセスしてUSBメモリで持ち出すケースもあり、USB接続履歴の調査が必要となります。

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

個人情報漏えいが起きたことが判明し、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。
個人情報漏えい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、USBメモリの接続履歴の調査、削除されたログの復元などのデジタル証拠の調査が行えず、不正アクセス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。

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情報漏えい調査実績

標的型メールを開封することで端末がウィルス感染

攻撃の踏み台とされたサーバーの復元調査

・背景

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。

・調査内容

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。

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

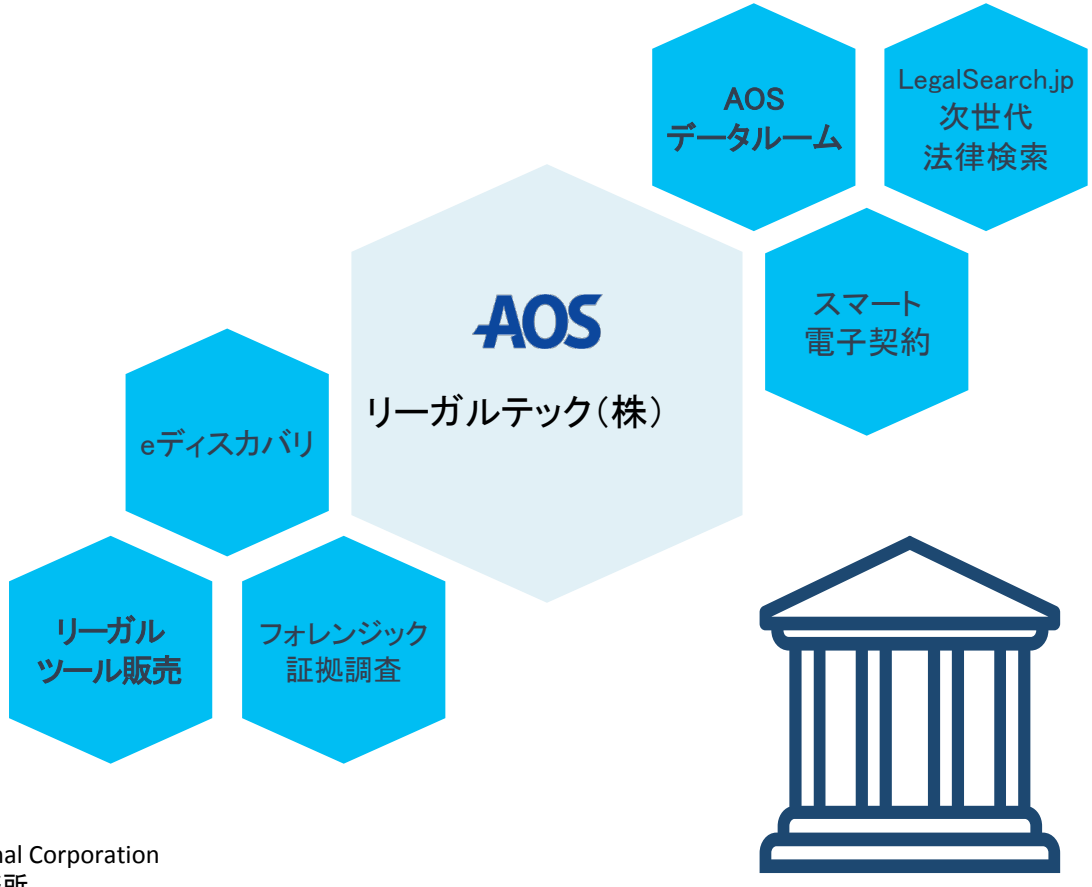
代表取締役 : 佐々木 隆仁

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