SMEレジリエンス 情報セキュリティ版 Vol.003

Resilience Information

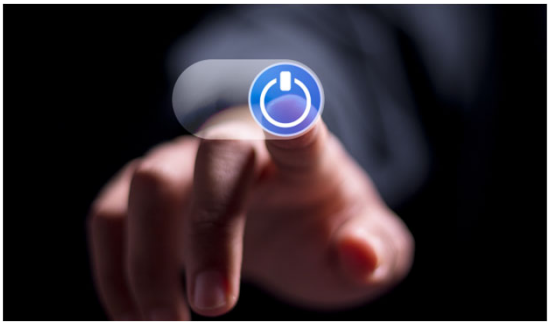
発信日:2025年10月8日 発信部署:中小企業セグメント営業部
リスクコンサルティングユニット
No.031-25-R010

企業が事業を行うなかで運用管理している情報資産は、取引企業情報、営業秘密情報、在庫データ、注文データ、経理情報、マニュアルや社員情報など多岐にわたり多くは機密情報となります。
業務利用しているPCやサーバーがマルウェアに感染したりすると、その際、どの情報が漏洩したか、どの情報が暗号化されたのか、など状況を把握し取引企業や関係者に対して、事実の説明や報告をする必要があり、それができないと、これまで積み上げてきた信用・信頼が失墜し、その結果、事業が継続できなくなる事態を招いてしまう可能性があります。

Q：
サイバー攻撃のおそれを感じた従業員がそのPCなどの端末に対して"すぐ行うべきこと"、"行ってはならないこと"、についてご存じですか？

マルウェア感染時に“電源オフは✕（Don't do that.）”

ネットワークから切り離し、電源オフはせず、ネットワークから隔離した上で、
専門のフォレンジック会社に調査を依頼するのが正しい初期対応です。



マルウェア感染時の正しい対応について

●ネットワークから隔離する

感染拡大を防ぐため、**LANケーブルを抜く**、**Wi-Fiを切断する**、などしてネットワークからPC端末等を隔離。

●電源は落とさない

メモリ（RAM）に保存されている情報を失わないために、PC端末等の電源は落とさず電源供給を維持。
※電源を切るとメモリ（RAM）の内容が消去されてしまうため、インシデントが発生した際は、電源を落とさずにメモリ内のデータを維持した上で、対応進める必要があります。

●専門家に調査依頼する

専門のフォレンジック調査会社へ調査依頼。

⇒ フォレンジック調査とは！（裏面へ）

●フォレンジック調査

フォレンジック調査は、調査対象により名称が異なり、主に以下のようなものなどがあります。

・**ディスクフォレンジック**とは、HDDやSSDのようなストレージを調査対象とするもの。

・**ネットワークフォレンジック**とは、パケットキャプチャやNetFlow、ProxyやFWのログのような通信情報を対象とするもの。

・**メモリフォレンジック**とは、メモリ（RAM：ランダムアクセスメモリ）という一時的な記憶装置を調査対象とするもの

迅速に被害の範囲や影響を把握し早期に対策を講じることは、被害の拡大防止と現状把握のために、フォレンジック調査は欠かせません。

“メモリフォレンジック”が重要な理由は、昨今の一部のマルウェアには、HDDやSSDのようなストレージドライブに痕跡を残さないようにつくられているもの（ファイルレスマルウェア）が存在するからです。メモリフォレンジックでは、メモリに残る情報を分析し、マルウェアの実行痕跡や不正なアクティビティに関する情報を取得することなどが可能です。

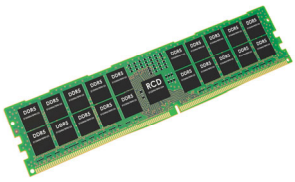
しかし

メモリに保存される情報は、電源が供給されている間はデータを保持することができますが、電源が切れるとメモリのデータは消去されてしまいます。

そのため、メモリフォレンジックで不正行為やハッキングなどの痕跡を収集する場合、シャットダウンせず、コンピュータの電源が入った状態で迅速に行う必要があります。

メモリには、OSやアプリの実行状態、ユーザーの操作履歴、ネットワーク通信の履歴など、コンピュータの動作に関する情報が一時的に保存されており、これらの情報を分析することで、他の調査方法では取得できない情報を取得することができます。

セキュリティインシデントとは、マルウェアの感染や不正アクセス、あるいは機密情報の流出など、セキュリティ上の脅威となる事象のことをいいますが、企業が事業活動を行っていくなかで、セキュリティインシデントが発生した場合は、発生した事象に関する情報の収集と分析、被害拡大などに向けた対策の実施、再発防止策の検討などを行ってください。PC端末などの取り扱いを間違えると、取引企業や社会からの信頼を失うことに繋がる可能性もあるため、ご注意ください。



AIG損害保険株式会社

TEL:03-6848-8500（大代表）

午前９時～午後5時（土・日・祝日・年末年始を除く）

https://www.aig.co.jp/sonpo

お問い合わせ・お申し込みは