Professional Security Services

インシデント発生時の被害の極小化と原因解明による再発防止支援

セキュリティインシデントが発生した場合、迅速な対応が被害を最小化する上で極めて重要です。近年、ランサムウェア被害やサプライチェーン攻撃が多発し、企業規模に関わらず顧客情報漏洩や事業停止といった深刻な被害をもたらしています。高度なセキュリティ対策を講じても、インシデントを完全に防ぐことは困難です。そのため、発生してしまったセキュリティインシデントの原因を特定し、適切な対策を講じることは、再発防止だけでなく、迅速な復旧を実現する上でも不可欠と言えます。

富士通では、マルウェアの感染やWebサイトの改ざん、大規模な標的型攻撃、ランサムウェア攻撃等、様々なセキュリティインシデントに対し、専門的な技術と豊富な調査経験を基に調査を実施し、被害の極小化と早期復旧を支援します。

参考
・NISTSP800-61:コンピュータインシデント対応ガイド

インシデント対応の鍵は「豊富な経験」

1 確かな対応力と技術力

金融、官公庁、製造業等、様々な業種に対応し、PC単体から大規模システムまで幅広い調査の経験を持つA3L（注1）所属の専門の調査員が調査を実施します。

2 多様な調査対象に対応

WindowsやLinuxサーバ・PC調査に加え、各種クラウドサービスの調査も対応可能です(注2)。

3 状況や目的に応じた調査方法の提供

セキュリティ侵害の根本原因と影響範囲を調査するセキュリティ侵害調査サービスに加え、マルウェア感染や不正アクセスの有無を早急に調査することを目的とした簡易調査（注3）も提供可能です。

（注1）A3L：FUJITSU Advanced Artifact Analysis Laboratoryの略称。高度なセキュリティ分析を行う専門機関として設立。
（注2）その他の機器についても、相談に応じて対応可否を検討します。
（注3）簡易調査：マルウェア感染や不正アクセス時によく見られる痕跡に限定した調査を実施し、短期間で調査結果を報告する方法。

対応支援例

- **不審なメールを開いてしまったため、影響の有無を確認したい**
- **マルウェアに感染した可能性があるため、影響を知りたい**
- **自社で管理するシステムに身に覚えのないファイルを発見したため、原因を知りたい**
- **外部から不正通信の連絡を受けたため、侵害の有無を調査したい**

サービスの流れ

事前準備
・セキュリティ侵害調査に必要なインシデント内容をヒアリング
・侵害調査の対象となる調査・分析対象データ、関連装置等の情報を受領

調査
・受領した調査・分析対象データ、関連装置等の情報をもとに、ディスクイメージ分析、ログ解析、マルウェア解析等を実施。被害範囲の特定、侵害の原因を調査

調査結果報告
・調査結果に基づき、原因・影響範囲・対策についてまとめた報告書を提出
・調査報告書の記載内容に関する報告会を実施(オプション)

メニュー体系

サービス名	備考
セキュリティ侵害調査サービス サーバ 基本サービス	Windowsサーバ、Linuxサーバ等を対象とした調査サービス
セキュリティ侵害調査サービス クライアント 基本サービス	クライアントPCを対象とした調査サービス
セキュリティ侵害調査サービス 報告会オプション	対面もしくはオンラインでの報告会を実施

本サービスは、経済産業省が定める「情報セキュリティサービス基準」に適合するサービスとして、情報セキュリティサービス基準適合サービスリストに登録されています。
関連リンク：
https://www.fujitsu.com/jp/solutions/business-technology/security/secure/news/security-service-standard.html

018-0016-30

お問い合わせ先

富士通株式会社
富士通コンタクトライン（総合窓口）0120-933-200
受付時間 : 9:00～12:00および13:00～17:30（土・日・祝日・当社指定の休業日を除く）
お問い合わせフォーム