ALSOK × 三井物産セキュアディレクション株式会社

Webサイトの情報漏えい・不正侵入等の事故対応・調査

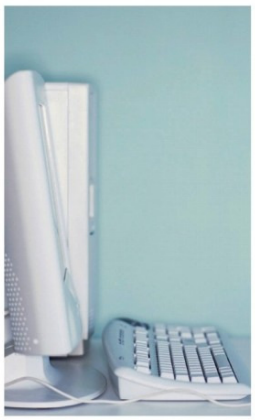
Information Leakage Investigation Service

情報漏えい調査サービス

情報漏えいなどのセキュリティ インシデントが起きたかも知れない……
その時、あなたの会社ではどう対応しますか？

顧客への対応方法はどうしたらよいか？ 事業継続性や損害賠償にかかわる問題に発展するのでは？など、ご担当者さまは多くの不安を感じることが現状です。このような状況下ではご担当者さまだけでの適切な判断・対応は難しく、初動対応を誤る危険性があります。特に初動対応では証跡データの保護など、作業における優先順位づけが重要となり、この判断を誤ることは今後の原因究明・対策案の検討に大きく影響を及ぼします。

以下のようなセキュリティ インシデントの兆候がある場合は、まずは ALSOK へご連絡ください。情報セキュリティの専門家である、三井物産セキュアディレクション株式会社（以下「MBSD」とする）と連携し対応いたします。



- 顧客から個人情報（ユーザー登録情報、クレジットカード情報）が漏えいしているとクレームを受けた
- 顧客から迷惑メールが届く様になったとクレームを受けた
- Webページが何者かによって改ざんをされた
- DoS攻撃などの不正パケットが増加した
- サーバに不審なファイルが出現した

セキュリティ インシデントが起きた場合、迅速かつ適切な判断・対応が重要!

『情報漏えい調査サービス』は、情報漏えいやデータ改ざんなどのセキュリティ インシデントにかかわる緊急事態に情報セキュリティの専門家である MBSD の Security Force※メンバー（セキュリティアナリスト）が 24 時間以内にお客さま先へ訪問し、セキュリティ インシデントの原因究明から恒久対策案の提示までを支援いたします。

- 24 時間以内に MBSD の Security Force メンバーが駆け付け
- 被害状況、暫定策、対策に関するマイルストーンなどの初動アドバイス
- フォレンジック技術を用いた本格調査 と 顧客・メディア対策支援
- セキュリティ監視による事業継続支援
- システム復旧から再発防止策などのフォローアップ

Security Force※
（セキュリティフォース）

Security Force（セキュリティフォース）とは、三井物産セキュアディレクション（以下、MBSD）のサイバーセキュリティの専門エキスパートチームのことです。

深い知識と高度なセキュリティ技術をもとに多数の事件・事故への対応実績を持つメンバーから構成されています。Security Force の主要任務は、通常のセキュリティ業者では対応しきれない事件の解決支援です。

例えばタイガーチームをご存知でしょうか。タイガーチームとは、米海軍が国防省の通信危機に対処するための部隊の名称です。タイガーチームによるテスト結果はセキュリティ侵害に対する、なかでも特に事後対応に有効活用されました。このタイガーチームのように、セキュリティ インシデントのための専任チームが MBSD の Security Force メンバーなのです。

Security Force のメンバーはセキュリティ インシデント対応に必要な「アプリケーション・サーバへの侵入」「ログ・マルウェア解析」「デジタルフォレンジック」などのノウハウを兼ねそなえています。

そして近年ではセキュリティ インシデントが起きた可能性のある「兆候」をもとに深刻な事態を判断、回避するための真実調査分析も行っています。また、サイバーテロをはじめ大規模な個人情報漏えい事件など、高度な技術と正確な対応を要する事件の発生にそなえ、世界中の情報を収集し、さまざまな攻撃手法を学び、かつ実践的な対応訓練も実施しています。

MBSD の Security Force メンバーは「情報漏えい調査サービス」を通じ、お客さまのセキュリティ インシデントにスピーディかつ丁寧にサポートいたします。

情報漏えい調査サービス

セキュリティインシデント発生！ お客さまよりお電話またはメールにてご連絡いただき、まずは事前ヒアリングで被害状況などを確認いたします。その後、MBSD の Security Force メンバーがお客さま先へ訪問し、以下サービスを提供いたします。

Ⅰ 初動調査

Ⅱ 本格調査

Ⅲ 顧客・メディア対策支援

Ⅳ 事業継続支援

Ⅴ 恒久対策案・フォローアップ

Ⅰ. 初動調査

お客さまよりご相談いただきましたセキュリティ インシデントにつきまして、MBSD の Security Force メンバーが現状調査から原因究明を行います。お客さま環境における被害状況、情報漏えいの有無、セキュリティリスクの有無を調査し、暫定策などを含めた初動アドバイスをいたします。

- ○ ハードディスク調査・分析作業
- ○ ハードディスク調査結果報告書の作成、提出
- ○ 現状調査（お客さまへのヒアリング）
- ○ 調査・分析作業
- ○ 初動アドバイス（暫定策、対策に関するマイルストーンについてご説明）
- ○ 初動調査報告書の作成、提出

Ⅱ. 本格調査

お客さまよりご相談いただきましたセキュリティ インシデントにつきまして、MBSD の Security Force メンバーがお客さま先にて証拠保全を行います。保全したデータを基に調査・分析作業を行い、お客さま環境における被害状況、情報漏えいの有無、セキュリティリスクの有無、恒久対策案などを含めご報告します。最終成果物として、“被害状況”、“想定される脅威”、“恒久対策案”、“マイルストーン”などをまとめた『本格調査報告書』を提供いたします。

- ○ 証拠保全作業
- ○ 調査・分析作業
- ○ 恒久対策案の提示
- ○ 本格調査報告書の作成、提出
- ○ 本格調査報告書をもとに報告会を実施
- ○ 証拠保全データの削除

Ⅲ. 顧客・メディア対策支援

顧客（お客さま、親会社、関係会社など）への説明、メディア、関係機関（監督官庁、警察など）への対策支援を実施します。お客さまには顧客への対応に専念していただき、必要となる説明文や質疑事項に対する回答などについては、MBSD のセキュリティコンサルタントが準備・支援いたします。また、お客さまの被害状況に応じて、関係機関への報告支援を実施します。

- ○ 対策本部の立ち上げ支援
- ○ 対策本部ご担当者さまへの対応支援
- ○ 顧客、メディア、関係機関への報告支援（説明文の作成支援、Q&A 問答集の提供）

Ⅳ. 事業継続支援

顧客（お客さま、親会社、関係会社など）保護を優先とした被害拡大防止策を実施します。お客さまのネットワーク環境に不正侵入検知装置を導入し、MBSD の Security Operation Center（以下、SOC）にてセキュリティ監視を行います。不正アクティビティ（不正侵入、不正操作など）を検知・防止することで、お客さまのビジネスを停止することなく事業の継続が可能となります。

- ○ 不正侵入検知装置の導入
- ○ MBSD の Security Operation Center（SOC）でのセキュリティ監視

Ⅴ. 恒久対策案・フォローアップ

本格調査で提示いたしました恒久対策案の支援を行います。セキュリティ インシデントの調査・分析結果に応じてフォローアップ内容は異なりますが、恒久対策となるシステム復旧支援をはじめ、セキュリティ強化支援や社員へのセキュリティ教育などを実施し、組織におけるセキュリティレベルの向上を図ります。

- ○ システム復旧支援
- ○ セキュリティ強化支援
- ○ 問合せ対応支援
- ○ 社員へのセキュリティ教育

サービス提供会社

M|B|S|D®

電話：03-5649-1981
電子メール：securityforce@mbsd.jp
http://www.mbsd.jp/
三井物産セキュアディレクション株式会社

サービスに関するお問い合わせ先

綜合警備保障株式会社
http://www.alsok.co.jp

ALways Security OK ALSOK

本社　〒107-8511　東京都港区元赤坂 1-6-6
TEL.　03-3470-5633（平日 9:00 ～ 18:00）
FAX.　03-3402-7663
電子メール：**inc-res@i-sec.alsok.co.jp**