

サイバーコネクトSHIG@

今、注目のサイバーセキュリティに関する情報をお届けします。

Cyber connect shig@

サイバー攻撃を受けたかもしれない時、どうしますか？

「インシデントハンドリング」とは？

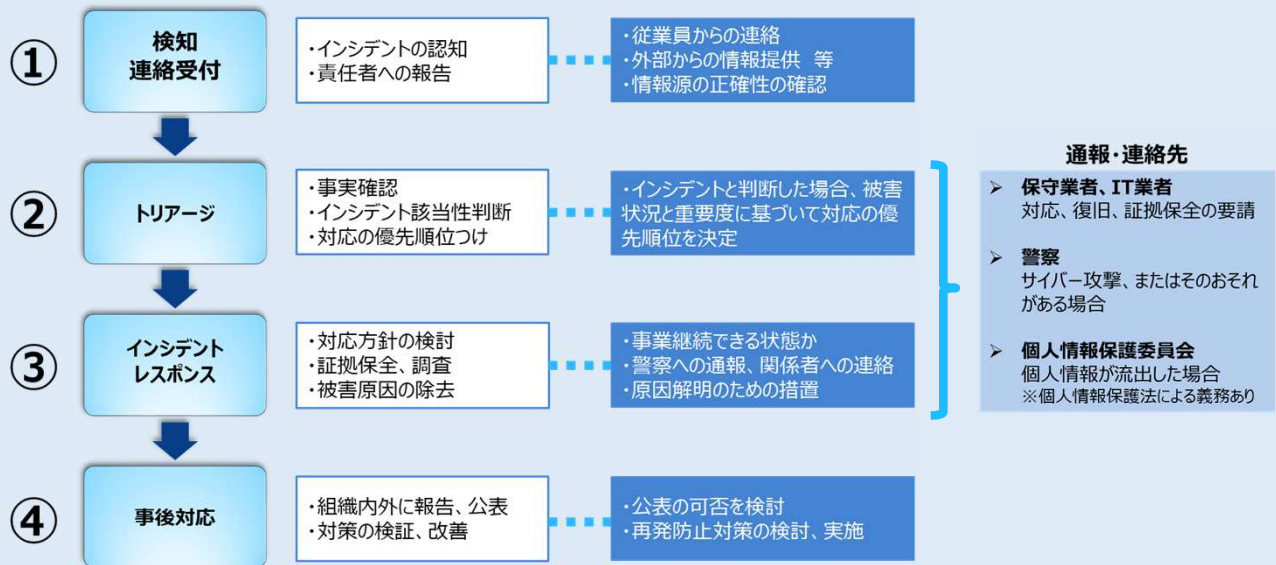


今や、サイバー攻撃については、完全に防御することは極めて困難とされています。万が一、サイバー攻撃を受けた場合に備えて対応要領を検討しておく必要があります。サイバー攻撃を放置したり、対応を誤ったりすると事業活動に大きな影響を与えます。攻撃を受けないための対策も重要ですが、**攻撃を受けた後の対応がより重要**になります。

インシデント（サイバー攻撃被害のほか人為的なミス等によるシステム障害も含む）が、発生した場合の対応要領のことを「インシデントハンドリング」といいます。インシデント発生時の対応を予め検討しておくことが重要です。



インシデントハンドリングの流れ（例）



インシデントハンドリングは、業種やセキュリティポリシーによって異なるため、自組織の考え方に基いて決定します。各報告先、通報先を確認しておくことが重要です。

参照：JPCERT/CC インシデントハンドリングマニュアル
https://www.jpCERT.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf

【サイバー攻撃を受けたかもしれない時の対処】

- すぐにネットワークを切断してください。
内部感染の拡大防止、外部への情報流出防止が重要です。
 - LANケーブル・・・端末から外してください。
 - Wi-Fi（無線）・・・ネットワークをオフにしてください。
- 電源は切らないでください。
 - メモリ上からデータが消えてしまい、調査ができなくなります。メモリには、外部への通信履歴が残っていることがあります。再起動もしないでください。

- ◆ インシデントは、発生することを前提に、予めインシデントハンドリングを検討しておきましょう。
- ◆ インシデントハンドリングに基づく訓練を実施しておく、発生時の対応がスムーズです。
- ◆ サイバー攻撃によるインシデントが発生した場合は、警察に通報してください。



← 公式X（エックス | 旧Twitter）でサイバーセキュリティ情報を発信中です。

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表） 県警webページ →

