滋賀県警察サイバーセキュリティ情報

サイバーコネクトSHIG@

R５年度 No.18

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）

①	検知 連絡受付	・インシデントの認知 ・責任者への報告	・従業員からの連絡 ・外部からの情報提供　等 ・情報源の正確性の確認
②	トリアージ	・事実確認 ・インシデント該当性判断 ・対応の優先順位つけ	・インシデントと判断した場合、被害状況と重要度に基づいて対応の優先順位を決定
③	インシデント レスポンス	・対応方針の検討 ・証拠保全、調査 ・被害原因の除去	・事業継続できる状態か ・警察への通報、関係者への連絡 ・原因解明のための措置
④	事後対応	・組織内外に報告、公表 ・対策の検証、改善	・公表の可否を検討 ・再発防止対策の検討、実施

通報・連絡先

- **保守業者、IT業者**
  対応、復旧、証拠保全の要請
- **警察**
  サイバー攻撃、またはそのおそれがある場合
- **個人情報保護委員会**
  個人情報が流出した場合
  ※個人情報保護法による義務あり

インシデントハンドリングは、業種やセキュリティーポシリーによって異なるため、自組織の考え方に基づいて決定します。
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と、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。
@shiga_cyber

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 →
https://www.pref.shiga.lg.jp/police/seikatu/304409/index.html