第１２号

F－CSNET NEWS

Fukuoka small and medium sized enterprises
Cyber security Support NETwork

平成３０年３月
【作成】福岡県警察本部
サイバー犯罪対策課

大事な顧客情報が漏えい？！会社の情報が漏えいしたらどうしたらいい？

情報漏えい発生時の対応ポイント

※　本記事は「コンピュータウイルス」や「不正アクセス」による情報漏えいを想定しています。

発見・報告

サイバー攻撃の発覚～
顧客のカード情報・メールアドレス・パスワード等の情報漏えい

コンピュータウイルスの発見は、ウイルス対策ソフトやメール等を受信した外部からの通知等により、また不正アクセスの発見はセキュリティ対策機器の警報等によって、それぞれ発見されることが多いようです。

（必要な措置の例）

- ○　経営者・実務責任者（システム管理者等）への報告
- ○　情報漏えい対応の体制の確保
  メンバーは、経営責任者・現場責任者・IT 担当者・社外の IT 委託先等

初動対応

原因と被害範囲の調査を自社で実施できるか判断

- ■　原因と被害範囲の調査を自社でできるかどうかを判断するなど、当面の対応方針を決定します。
- ■　被害の拡大、二次被害のための応急措置を行います。
  証拠を消してしまわないように注意！

（応急措置の例）

- ○　ウイルス感染したパソコンのネットワークからの切り離し
- ○　不正アクセスを受けた機器（サイト）のネットワークからの切り離し
- ○　不正アクセスを受けた機器（サイト）の停止

調　査

原因と被害範囲の調査をセキュリティ会社に依頼することも検討

適切な対応についての判断を行うため、５Ｗ１Ｈ
（いつ、どこで、誰が、何を、なぜ、どうしたのか）
の観点で調査し、情報を整理します。

（整理すべき情報）

- ○　漏えいした情報は何か？（個人情報か？公共性が高いものか？）
- ○　情報へのセキュリティ対策は何をしていたのか？
- ○　影響はどこにあるのか？（個人か？公共インフラか？企業か？）
- ○　管理上の問題点はどこか？

通知・報告・公表　個人情報の本人、取引先等への通知、監督官庁、警察等への届出、ホームページ等による公表

抑制措置と復旧　被害の拡大防止、再発防止の取組、停止したサービス・アカウント等の復旧

事　後　対　応　抜本的な再発防止策の検討・実施、被害者に対する損害の補償等

詳しくは ⇨ 参照元 IPA（独立行政法人情報処理推進機構）「情報漏えい発生時の対応ポイント集」
https://www.ipa.go.jp/security/awareness/johorouei/index.html

イラストについては、東京都発行「中小企業向けサイバーセキュリティ対策の極意」P143、P155～P157 から引用
www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/jigyou/guidebook/index.html#policy