SEAGULL 通信

令和元年12月26日発行

No. 9

"security action for guarding technical intelligence"

あなたの会社はルールを守れていますか？

情報流出が起きた想定

A社では、セキュリティを導入していたものの、秘密情報に関する社内規程が無視され、共有サーバーに秘密情報を保存するという社内規程違反が常態化していた。そのような状況下、A社職員宛に取引先を装った「標的型攻撃メール」が届き、メール本文の文字化けに違和感を持ったものの同職員は報告せず放置した。その結果、ウイルスに感染した当該職員の端末を通じて、社内複数の端末へと感染が拡大し、共有サーバーに保存された秘密情報等が盗まれる被害に遭った。

社内規程

- **取扱方法**
  - ○ 秘密情報が記録されたファイルは共有サーバーに原則保存禁止
  - ○ 保存が必要な場合はパスワード等の設定が必要
- **受信メール**
  - ○ 不審メールを受信した場合はシステム担当者へ報告し、組織で対応

被害が拡大した原因と対策

管理体制

① 共有サーバーに秘密情報が安易に保存されるなど、社内規程の無視を常態化させてしまった。

対策 ➡ 社内規程が遵守される職場の環境づくり。
（心理的抑制による対策～SEAGULL通信№7参照）

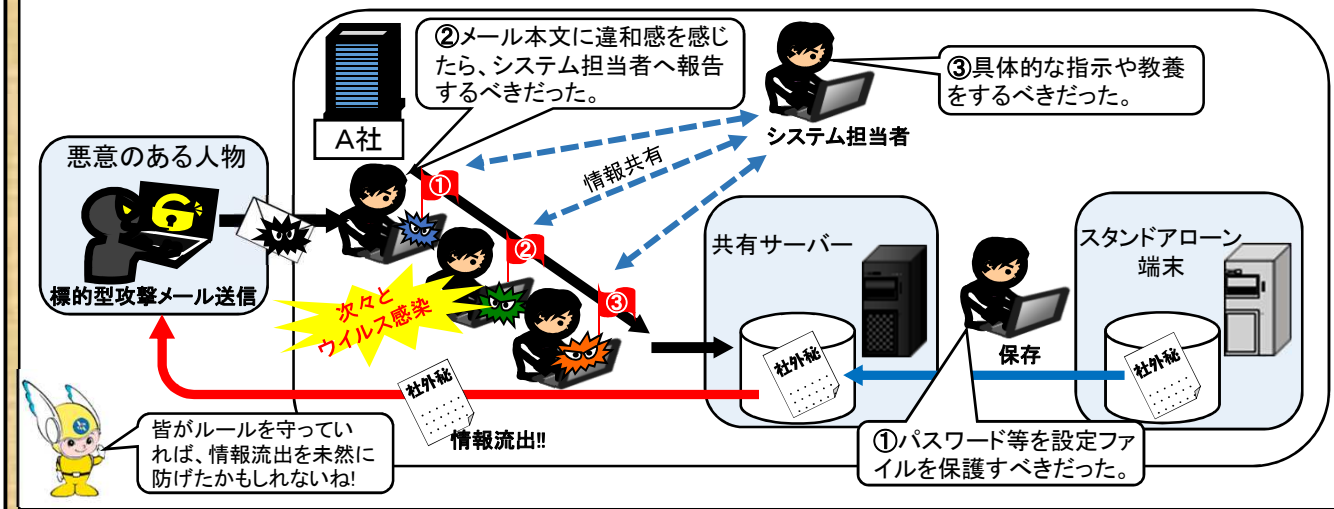
社内の対応

② 不審メールの受信を安易に考えて、システム担当者への報告を放置した。

対策 ➡ 従業員に対する対処への理解向上のため、不審メールを装って、実際に従業員へ不審メールを送信し 、開封率を確認する参加型の訓練等を実施。

③ システム担当者から不審メールの詳細について、情報共有や具体的な指示がされず対応が遅れた。

対策 ➡ システム担当者は、高度化・巧妙化するサイバー攻撃の実情を踏まえ、従業員に定期的に教養を実施。



～秘密情報を守るためできること～

年々、高度化・巧妙化するサイバー攻撃に対し、完璧な防御策はないと言われています。

つまり、いかにして被害を**最小限**にするかが企業の課題となってきます。各企業の情勢に応じて**セキュリティー教育**を実践し、**「ルールを守る意識付け」**を徹底しましょう。

しーがる川柳

社内規程　行き届いているか　我が会社

SEAGULL事務局

▼ SEAGULL事務局（外事課内） ▼

〒231-8403　横浜市中区海岸通2丁目4番　神奈川県警察本部

相談窓口　Email：seagull@police.pref.kanagawa.jp