SEAGULL 通信

令和元年６月14日発行

No. 5

"security action for guarding technical intelligence"

あなたの会社にも不審なＥメールが届いているかも・・・

"ヒヤリハット" 事例（情報漏洩編）

《A県所在の繊維メーカーB社》

製造部門の従業員宛に顧客を装ったEメールが届いたが、その内容に違和感を覚えたため、**添付ファイルを開かずに社内セキュリティ部門に相談**しました。

調査の結果、コンピュータウィルスが仕込まれた"**標的型攻撃メール**"であることが判明し、会社の機密情報の流出を未然に防ぐことができました。

標的型攻撃メールを御存じですか？

スパムメール等のいわゆる「迷惑メール」とは違い、会社の秘密情報等を盗むことを目的として**取引先の関係者等になりすまして**、あたかも**業務に関係しそうなEメール**を送信し、又は**何度かEメールのやりとりをして信頼させ**た後、コンピュータウィルスを仕込んだ添付ファイルを送り付ける手法です。

こんなメールに…

注意！

・知らない人からのメールだけど、業務に関係しているし、興味をそそる内容だし・・・。
・何度かやり取りのある人からのメールだけど、自然を装って本文のURLや添付ファイルを開かせようとしている・・・。
・取引先からのメールなのに、よく見たらフリーメールのアドレスが使われている・・・。
・日本語が不自然だな・・・。本文のフォントが何かおかしい（文字化け等）・・・。

ちょっとでも不審に思ったら、添付ファイルを開かないで、相手の人に電話で問い合わせることも大事だね!!

SEAGULL通信からのアドバイス

「標的型攻撃メールへの対策」について

① 可能な限り、外部ネットワークにつながらない機器に秘密情報を保存する。
② 外部ネットワークにつながったPC等に秘密情報を保管する場合は、「ファイアーウォール、アンチウィルスソフト」を導入し、OSやソフトウェアのアップデートをしっかり行う。
③ 秘密情報の電子データを暗号化する。（あくまで一例です）

しーがる川柳

アクセス権　過剰付与は　命取り

警察署SEAGULL担当 T.Kさん

しーがる川柳公募中!!
SEAGULL通信で紹介させていただきます。

▼ 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