毎月1回の“知ってるだけで対策がとれる”セキュリティ情報

サンエイすてーしょん

お客様各位

（社内への周知・回覧をお願いします）

※以前名刺交換をさせて頂きましたお客様に情報提供をさせて頂いております。

拝啓　時下ますますご清栄のこととお喜び申し上げます。平素は格別のご高配を賜り誠にありがとうございます。

今号から3部に分けて、『情報セキュリティに全社で取り組まなければならない理由』についてご案内いたします。

『情報セキュリティに全社で取り組まなければならない理由』 第1部

「1人のミスが命取り！ 疑われるのは会社の体質です」

昨今、社員の不注意などのミスにより、会社の信頼を損なうような事例が発生しています。**たった1人**が不用意にウイルスに感染してしまうだけで、社内ネットワークへ攻撃者の侵入を許してしまい、**会社全体に被害が及んでしまうことがあります**。そうならない為にも、社員全員が適正な対処力を身につけるよう、注意していく必要があります。

事例：大手旅行会社を襲った標的型攻撃の巧妙な手口

2016年、大手旅行会社から約793万件もの情報漏えいが起こった事件は、取引先を装ったメールの添付ファイルを従業員の1人が開封してしまったことが原因でした。そのメールは実在する取引先の会社・部署や担当者の署名があり、添付ファイルも社内でよく使う表記のタイトルがついたPDFでした。メールアドレスのドメインも実在する取引先企業のもので、少し見ただけでは気づかれない巧妙な手口が使われていました。

こうした「企業などに偽メールを送りつけ、ウイルスに感染させて情報流出を狙う手口」を標的型攻撃と呼びます。メールの本文で受信者を騙し、添付ファイルを開かせようとしたり、本文中のURLをクリックさせようとします。その添付ファイルや不正サイトからマルウェアに感染する仕組みとなっています。

このような攻撃からの被害を防ぐためには、不用意に添付ファイルやメール本文中のURLをクリックしないなど、常に注意をしておくことが求められます。しかし、これらを理解していても、必ずしも正しい行動がとれるかは分かりません。標的型攻撃は常に進化し、メール本文はとても巧妙になっています。進化するサイバー攻撃に対応できるように、**社員に向けての定期的な社内研修を行うことが求められます。**（先月号「新しいサイバー攻撃の情報を共有しよう」参照）

また、誰かが標的型攻撃メールを開いてしまった場合、開封後の影響を最小限に抑えるための環境を整備しておくことも必要です。具体的には、**誤って悪意のあるファイルを開いてしまったり、リンクをクリックしたことに気付いた場合、すぐにセキュリティの担当者に連絡するルールを作っておくことや、メールチェックを行い攻撃を未然に防ぐようなシステムを入れることなどです**。社内のルール作りと、設備対策が大切です。

これまでのFAX「サンエイすてーしょん」は弊社ホームページにも掲載しております。新入社員向けの研修としてもぜひご活用ください。

敬具

社内回覧確認枠

発行：株式会社サンエイ
電話：084-922-6190
FAX：0120-22-6190

□ 今後情報提供が**不要**な場合はチェックを頂きご返信ください。

御社名：＿＿＿＿＿＿＿＿＿＿