中小企業の

セキュリティー対策

—38—

新型コロナ関連の偽メールに警戒を

ビジネスメール詐欺 国内企業も標的に

独立行政法人情報処理推進機構（IPA）は4月27日、ビジネスメール詐欺に関する3度目の注意喚起を行った。

ビジネスメール詐欺とは、巧妙に細工したメールのやりとりで企業の担当者をだまし、攻撃者の用意した口座へ送金させる詐欺の手口である。その多くは日本企業の海外支社などが標的となっている傾向があるが、日本語の偽メールで国内企業が直接狙われる事例も確認している。

3月には、ある国内企業のCEOを詐称し、その複数のグループ会社のCEOを標的としたビジネスメール詐欺を確認している。日本語に不自然な点が少ないだけでなく、受信したうちの1社がこのメールに返信したところ、攻撃者から続けて日本語で返信が送られてきている。

また、3月と4月に新型コロナウイルス感染症（COVID—19）を話題とした英文のビジネスメール詐欺も複数確認している。メールの内容は、これまでIPAで多く確認してきた事例同様、何らか機密性の高い財務処理が必要であると称するものであった。返信をした場合、何らかの口実とともに、攻撃者の口座への送金依頼に話が進むものと思われる。現在、あらゆる企業が困難な状況にあり、予定外の対応も多く発生している状況ではあるが、これらを悪用するような口実にだまされないよう、注意が必要である。

ビジネスメール詐欺は、手口が悪質・巧妙なだけでなく、金銭被害が多額になる傾向がある。改めて、企業が相対している敵は「偽メール」ではなく、そのメールを送り付けている攻撃者（人間）であり、その攻撃者は手口をアップデートしながら、複数の企業へ向け執拗（しつよう）に攻撃を繰り返しているという認識が重要である。一見、メールが偽物であると見破ることが容易に思えたとしても、攻撃者を侮るべきではない。IPAには、15年から約5年間にわたり、ビジネスメール詐欺の情報が継続的に寄せられている。メール文面の日本語化などによって、あらゆる国内企業において、引き続き注意を要する状況である。

従業員に注意喚起し対策を講じる

ビジネスメール詐欺は、メールのなりすましなどのサイバー攻撃の手法を用いつつ、巧妙に人をだます手口である。システムやセキュリティーソフトによる機械的な防御、偽メールの排除が難しいことが、被害抑止を難しくしている。従って、まずは従業員へ、このような詐欺の手口があるということを知らせる必要がある。その上で、次のような対策を行うことが望ましい。

■普段と異なるメールに注意

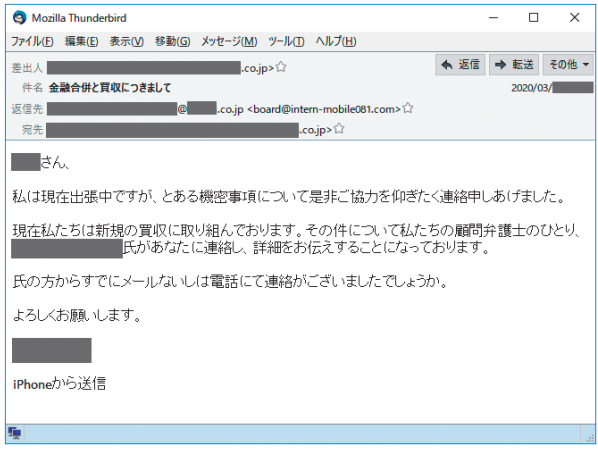
不審なメールは社内で情報共有する。

■チェック体制の整備

急な振込先や決済手段の変更などが発生した場合、取引先へメール以外の方法で確認する。

■ウイルス・不正アクセス対策

セキュリティーソフトを導入し、最新の状態にする。また、メールアカウントに推測されにくい複雑なパスワードを設定し、他のサービスとの使い回しをしない。メールシステムでの多要素認証、アクセス制限の導入を検討する。



日本語のビジネスメール詐欺のメール

ビジネスメール詐欺に関する注意喚起や対策の詳細はIPAのWebサイト（QRコードを参照）を確認してほしい。

（独立行政法人情報処理推進機構・江島将和）