法人口座におけるインターネットバンキング不正送金事犯に対する注意喚起のお願いについて

最近、一般企業の法人口座資金を狙った、フィッシングによるインターネットバンキング不正送金事犯の被害が立て続けに発生しているため、下記のとおり情報共有いたします。皆様におかれましては、関係企業に対して注意喚起していただくようお願い申し上げます。

記

○　発生事例

銀行を騙った者から一般企業宛てに電話連絡があった後、フィッシングメールが送られてくる事例

①　A会社にB銀行担当者を名乗る者（以下「犯人」という。）から電話がかかってきた（先立って銀行名を騙った自動音声の電話がかかってくる場合もあり）。

②　犯人から「インターネットバンキングの電子証明の期限が切れているので更新してもらいたい。これからメールでURLを送信するので、メールアドレスを教えてほしい。」と言われたので、A会社担当者はメールアドレスを教えた。

③　その後、A会社宛てにリンクが書かれたメール（フィッシングメール）が届いた（犯人との通話は継続している状態）。

④　A会社担当者がそのメールに書かれたリンクをクリックすると、IDやパスワードを入力する画面（フィッシングサイト）が表示された。

⑤　犯人の電話指示に従い、A会社担当者が契約者番号・ID・パスワードを入力すると、次に取引実行パスワードやワンタイムパスワードを入力する画面が表示された。

⑥　さらに犯人の電話指示に従い、A会社担当者がワンタイムパスワードを入力すると、犯人から「手続きは終了した。」と言われ、通話を終えた。

⑦　その後、A会社担当者がA会社の口座残高を確認すると、資金がA会社と全く無関係の法人口座へ不正送金されていることが判明した。

○　注意喚起していただきたい事項

金融機関が顧客企業に対して、メールアドレス等を聴取することは、基本的にはないことを御周知いただくとともに、以下について注意喚起をお願い申し上げます。

(1)　銀行担当者を名乗る者から電話があった際は、担当者の部署・氏名等を聞いた上、銀行の代表番号から担当者に折り返し連絡するなど、慎重に対応すること。

(2)　メール等に記載されているリンクをクリックしたり、QRコードを読み取ったりして、フィッシングサイトにアクセスしないこと。

(3)　被害が発生してしまった場合は、企業所在地管轄の警察署に相談すること。