Ksisnetだより
発行:Ksisnet事務局
令和元年9月27日
Vol.67

「情報セキュリティ10大脅威2019」（組織）
2位　ビジネスメール詐欺による被害

ＩPA（情報処理推進機構）から、「情報セキュリティ10大脅威2019」が公開されています。「組織」の視点からは、昨年３位の、
「ビジネスメール詐欺による被害」
が脅威の２位として選出されています。

ビジネスメール詐欺（BEC）は、取引先や経営者とやりとりするようなビジネスメールを装い、巧妙に細工されたメールのやりとりで企業の金銭を取り扱う担当者を騙し、攻撃者（犯人）の用意した口座へ送金させる詐欺の手口です。

順位	組織	昨年順位
１位	標的型攻撃による被害	１位
２位	ビジネスメール詐欺による被害	３位
３位	ランサムウェアによる被害	２位
４位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
５位	内部不正による情報漏えい	８位
６位	サービス妨害攻撃によるサービスの停止	９位
７位	インターネットサービスからの個人情報の窃取	６位
８位	ＩｏＴ機器の脆弱性の顕在化	７位
９位	脆弱性対策情報の公開に伴う悪用増加	４位
10位	不注意による情報漏えい	12位

「NEW」は初めてランクインした脅威

＜攻撃手口＞

○取引先との請求書の偽装

取引先と請求に係るやりとりをメールで行っている際に、攻撃者（犯人）が取引先になりすまし、攻撃者（犯人）の用意した口座に差し替えた偽の請求書等を送りつけ、振り込ませます。なお、攻撃者（犯人）は取引のやりとりや関係している従業員の情報をなんらかの方法により入手した上で攻撃を行っています。

○経営者等へのなりすまし

企業の経営者等になりすまし、従業員に攻撃者（犯人）の用意した口座へ振り込ませます。このとき、攻撃者（犯人）は事前に入手した、経営者や関係している従業員の情報を利用し、通常の社内メールであるかのように偽装します。

○窃取メールアカウントの悪用

従業員のメールアカウントを窃取し、アカウントを乗っ取った上で、その従業員の取引実績のある別の企業の担当者へ、攻撃者（犯人）の用意した口座を記入した偽の請求書等を送りつけ、振り込ませます。
メール本文は巧妙に偽装され、送信元が本物のアカウントであるため、受信したメールが攻撃であることに気づきにくい。

○社外の権威ある第三者へのなりすまし

弁護士や法律事務所といった社外の権威ある第三者へなりすまし、企業の財務担当者等に対して、攻撃者（犯人）の用意した口座へ振り込ませます。

○詐欺の準備行為と思われる情報の窃取

詐欺を実行する前の準備行為として、標的組織の情報を窃取する場合があります。
例えば、攻撃者（犯人）が詐欺の標的とする企業の経営者や経営幹部、または人事担当等の特定任務を担う従業員になりすまし、企業内の他の従業員の個人情報等を窃取します。

（IPA「『情報セキュリティ10大驚異2019』を決定」を基に作成）

「情報セキュリティ10大脅威 2019」の詳細については、下記ウェブサイトで公開されています。 https://www.ipa.go.jp/security/vuln/10threats2019.html

対策／対応

● 被害の予防（被害に備えた対策含む）

①「情報セキュリティ対策の基本」（※１）を実施

＜メールの真正性の確認＞

①メール以外の方法で事実確認
振込先の口座変更等がある場合、電話やFAX等メール以外の方法で取引先に確認する。

②普段とは異なるメールに注意
普段とは異なる言い回しや、表現の誤り、送信元のメールドメインに注意する。

③過剰に判断を急がせるメールに注意
至急の対応を要求するなど、担当者が真偽を確認する時間を与えないようにする手口も考えられる。真偽を確認するフローを事前に策定するなど準備をしておく。

④電子署名の付与
取引先との間で請求書等の重要情報をメールで取り扱う場合は電子署名によるなりすまし防止の対策も有効である。

＜メールアカウントの適切な管理＞

①ビジネスメール詐欺では、攻撃や被害に遭う前に、何らかの方法でメールが盗み見られている場合があるため、パスワードの適切な管理やログイン通知機能等で不正ログイン対策を行う。

● 被害を受けた後の対応

①CSIRT（※２）への連絡　③踏み台や詐称されている組織への連絡
②警察に相談　④影響調査および原因の追究、対策の強化

CSIRT（※２）･･･企業や行政機関などの組織内に設置され、コンピュータシステムやインターネットなどのネットワークに保安上の問題や事故が生じた際に対応する専門チームのこと。

「情報セキュリティ対策の基本」（※１）

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

参考　ＩＰＡ（情報処理推進機構）