**サイバーセキュリティ相談対応の傾向【2018年度】**

2019年4月12日

サイバーセキュリティ担当

サイバーセキュリティ対策の相談窓口開設以来の相談の内容を分類し傾向を調査したもの

# 全体傾向

* 今年度は、昨年度と同様に、「ECサイトのなりすまし被害」の相談が多く寄せられている。
* BEC(ビジネスメール詐欺)について、海外と取引している中小企業からのセキュリティ被害の問合わせが増加している。
* また、詐欺被害に繋がりかねない「迷惑メール・スパムメール」が急増している。

# 分類別傾向

* 個別サイバーセキュリティ事象の相談（「実際に被害にあった（侵害の予兆を含む）」、「事前の対策（事象毎の予防策）」）、「サイバーセキュリティに関する組織的な対応策」、「その他」で分類すると、個別サイバーセキュリティ事象の被害相談が6割強を占める。

## 個別サイバーセキュリティ事象の相談【実際に被害にあった（侵害の予兆を含む）、「事前の対策（事象毎の予防策）】

* 最も多いのは、「フィッシング詐欺・なりすまし」である。
  + 「なりすまされたECサイトからの被害相談」が大半で、「なりすまされたECサイトの利用者からの被害相談」はわずかである。
* 2017年度まで多かった「マルウェア（ウイルス）による被害相談」で、ウイルス感染のうち「ランサムウェアを使った詐欺・恐喝」の直接の相談は少なかった。
* 「マルウェア（ウイルス）による被害相談」の中には、「アドウェアによる詐欺」も僅かであるが寄せられた。
* 次に「迷惑メール・スパムメール」が3割強で、「あなたのデバイスをハッキングし、あなたがポルノサイトを閲覧している様子を記録した。コンテンツを知り合いにばらまかれたくなければBitcoinで〇〇ドル支払え」というような「セクストーションを装い、仮想通貨を要求するスパムメール」が増加している。

## 「サイバーセキュリティに関する組織的な対応策」

* 「サイバーセキュリティ対策の導入」の方法に関する相談は2割弱であり、あまり多くはない。しかし、経営課題としてのサイバーセキュリティのリスク管理への取り組みについて、経営者層からの相談が複数件あった。
* 組織的な対応策として、全般的な対策、管理的、人的、技術的、物理的対策に分類するとそのうち、具体的な技術対策が半数を占める。

# TCYSSとしてパフォーマンス

* サイバーセキュリティ対策として、インシデント発生時に早期の検知と被害の拡大を防止することが特に重要である。
* ポータルサイトにおいて、東京都発行の小冊子「中小企業向けサイバーセキュリティ対策の極意」の追補版として、サイバーセキュリティ侵害に関する新たな事象と予防策、各関係機関が提供しているガイドラインの情報等を整理して発信していく。
* 中小企業のセキュリティ侵害により、サプライチェーン全体に被害が広がることや、攻撃者の踏み台として悪用される可能性がある。特に中小企業の経営者へのサイバーセキュリティ啓発や、情報共有を継続的に行っていく必要がある。

# 2019年度に実施すべきと思われること（案）

## サイバーセキュリティ関連情報の収集・蓄積（情報の知識化）

* 「中小企業向けサイバーセキュリティ対策の極意」の解説書及び内容の改訂
  + サイバーセキュリティ経営ガイドラインの重要10項目の改訂対応
    - サプライチェーン
  + ブロックチェーン
  + 総務省、NICTのNotice対応
  + なりすましECサイト対策
  + IoTセキュリティ、クラウドセキュリティ
  + 守りのIT投資
    - 事業継続計画（BCP）の一環としてのサイバーセキュリティ対策（明文化）
    - テレワークソリューション（Wifiネットワークセキュリティ）
    - 法律違反の可能性への対応方法の解説
      * GDPR対応
      * 個人情報保護法改正への対応
  + 攻めのIT投資
    - AIが人を支援するインテリジェント・ワークプレイスの活用におけるサイバーセキュリティ対策
      * Society5.0, Connected Industry, DX, CPS対応
      * IoT、ビッグデータ、機械学習、クラウドサービス等の活用におけるサイバーセキュリティ対策
    - サイバー・フィジカル・セキュリティ対策フレームワーク対応
      * サプライチェーン全体での対策（中小企業向け）
  + 関連情報、参考文献の充実
* 外部プレゼンテーション用資料の作成
* セキュリティ関連機関のドキュメントのキャッチアップ
  + NIST SPシリーズ
  + JPCERT, USCERT
* 業務ハンドブック【専門員用】の更新⇒打ち合わせ後に、対応マニュアルだけでなく、ハンドブック全体を追加
  + 第1編　はじめに
  + 第2編　相談対応マニュアル（相談対応時参照用）
    - 案件別対応手順【専門員用】
    - インシデント対応フロー及び解説【相談者向け】
  + 第3編　個別調査分析資料（知見の蓄積）
    - セミナー等での情報収集・整理
  + 第4編次世代技術の実践習得
    - 先進技術の実践によるノウハウ習得
  + 第5編　実践的なノウハウ・知識の提供用資料（知見の発信）
  + 付録

## サイバーセキュリティ関連情報の発信の充実（知識の提供）

* ポータルサイト、SNS等での発信
  + 中小企業に伝えたいホットな情報
    - ⇒トピックに載せて、産業労働局のTwitterへ
* 「中小企業向けサイバーセキュリティ対策の極意」の追補情報の発信
  + ポータルサイトで「中小企業向けサイバーセキュリティ対策の極意」の追補情報、解説情報の発信
    - 「中小企業向けサイバーセキュリティ対策の極意の解説書及び内容の改訂」で収集・蓄積した情報をもとに、デザイン、編集、コピーライト業務を外部に委託する。
  + 2020年度、「中小企業向けサイバーセキュリティ対策の極意」の改訂版を電子書籍で発行、予算が付けば、冊子体も発行
* 外部プレゼンテーション、出張相談⇒各種セミナーで相談受付だけでなく、プレゼンの時間も確保

## サイバーセキュリティ基本法に基づいた「サイバーセキュリティ協議会」への参画⇒総会の議題に

* 第一類、第二類、一般構成員のどのレベルかは要検討
* NISC、IPAとの情報交換及び連携
  + インターネットでは公開されていないセキュリティ関連情報の共有
  + IPAセキュリティセンターとのホットライン
* 警視庁、TCYSSメンバーとの情報交換及び連携
  + Yammer等の情報共有ツールの利用促進