

情報セキュリティ 10 大脅威 2020

情報セキュリティ 10 大脅威 2020 - IPA

順位	組織	昨年順位
1位	標的型攻撃による機密情報の窃取	1位
2位	内部不正による情報漏えい	5位
3位	ビジネスメール詐欺による金銭被害	2位
4位	サプライチェーンの弱点を悪用した攻撃	4位
5位	ランサムウェアによる被害	3位
6位	予期せぬIT基盤の障害に伴う業務停止	16位
7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスからの個人情報の窃取	7位
9位	IoT機器の不正利用	8位
10位	サービス妨害攻撃によるサービスの停止	6位

(出典：IPA 独立行政法人情報処理推進機構 <https://www.ipa.go.jp/files/000080080.pdf> より抜粋)

IPA（独立行政法人情報処理推進機構）より、「情報セキュリティ 10 大脅威 2020」が決定され公開されています。

これは、2019年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約140名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い決定されたもので、個人と組織について順位が公開されています。

個人は、キャッシュレス決済や消費税増税などに関連するポイント還元などでスマホ決済が多くなり、その決済方法の不備などから利用者が被害に遭うなど「スマホ決済の不正利用」が、初めてランクインして1位でした。

対して、組織に対する脅威では、昨年同様「標的型攻撃による機密情報の窃取」が1位となり、2位は3ランクアップで「内部不正による情報漏えい」でした。2019年末には、ある県庁で個人情報や機密情報を含む行政文書の保存に使用されていたハードディスクドライブ（HDD）が、オークションで転売され、個人情報の漏えいが大問題となりました。問題のHDDは、県の共有サーバから取り外し、リース契約をしていたリース会社へは簡易的な削除が行われて引き渡され、その後契約に基づいたHDDの処分を別の処理会社の丸投げされ、同社の消去担当者が、その一部を不正に持ち出しオークションサイトに転売していた事件です。共有サーバは、データの暗号化がされておらず、県は「データ復旧が不可能とされている方法によりデータ消去作業を行うものとする」という契約について、リース会社からも消去証明書の提出を受けておらず、リース会社は、外部の処理会社に対して「HDDはデータを専用ソフトで消去、動作しないHDDは物理破壊」という内容の契約をしているにもかかわらず、完了報告も要求せず、その処理会社ではHDD廃棄に関し、物理破壊を行う際のダブルチェックも行われていませんでした。

6位の「予期せぬIT基盤の障害に伴う業務停止」については、2019年8月には空調設備の管理システム障害が原因で、某クラウド事業者で大規模なシステム障害が発生したり、12月にはある会社の自治体向けクラウドが停止したため、47自治体などのシステムが一齐にダウンし、業務や住民サービスに影響が出たりしました。また、台風など大規模自然災害の影響も多大だったため、昨年の16位という圏外から大幅にランクアップしました。

情報セキュリティ 10 大脅威は、毎年IPAより公開されているので、セキュリティのトレンドや、新しいセキュリティ対策技術を習得する上でも、どのような脅威が上位を占めているのか、常にウオッチしておくべきです。