2021 年 6 月 21 日
デジタルアーツ株式会社

PRESS RELEASE

＜2020 年にインシデントのあったテレワーク導入組織のセキュリティ対策を調査＞
セキュリティインシデントの 8 割以上が Web アクセスとメールに起因
テレワーク導入組織はインシデントを経験しつつも、テレワーク継続意向は 100%
～テレワーク恒久化に向け、メールと Web を使う攻撃に合わせた入口対策が改めて重要に～

情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、全国の民間企業や官公庁の IT システム・情報セキュリティ担当者 1,065 名を対象に、「テレワーク導入・導入検討中の組織に対するセキュリティ対策意識調査」を実施しました。

テレワークの導入は新型コロナウイルス感染症拡大の影響で急速に進みましたが、同時にセキュリティ対策が不十分なテレワーク環境を狙ったサイバー攻撃も増加しています。このような背景を踏まえ、テレワーク実施組織によるセキュリティインシデント（保安上の脅威となる事象、以下インシデントとする）の発生状況やセキュリティ対策に対する意識と現状の実施状況について調査しました。調査対象は、自組織のインシデント状況を把握し情報セキュリティ対策の意思決定に関わり、かつ、2020 年 1 月～12 月に何らかのインシデントが発生した組織としています。

セキュリティインシデントの 8 割以上がフィッシングメールや不正サイトへのアクセスなど Web アクセスとメールに起因

全国の民間企業や官公庁の IT システム・情報セキュリティ担当者 1,065 名を対象に、2020 年に組織内でどのようなインシデントが発生したかを調査したところ、インシデントの 8 割以上が Web アクセスとメールに起因していることがわかりました。最近では元職員による営業秘密の持ち出しなど内部不正も話題になりましたが、依然として内部攻撃よりも外部攻撃のインシデントが多いことが明らかになりました。

Web アクセスとメールに起因するインシデント件数　**2,782** 件（**83.4%**※）　／　**全体のインシデント件数　3,334 件**

＜＜セキュリティインシデントの内訳＞＞

フィッシングメールの受信	695 件	サービス妨害（Dos/DDos）攻撃	179 件
ビジネスメール詐欺のメール受信	534 件	内部不正による情報漏洩（職員の情報持ち出し等）	177 件
不正サイトへのアクセス	395 件	**Emotet 等マルウェア感染**	124 件
メール誤送信など意図しない情報漏洩	380 件	サプライチェーンの弱点を悪用した攻撃	98 件
標的型攻撃	345 件	自社サイトの改ざん	81 件
ランサムウェア感染	309 件	その他	17 件

※回答者 1,065 名に対し、2020 年に組織内で発生したインシデントを複数回答可で尋ねたところ、全体の回答数が 3,334 件であった。このうち、不正メールの受信・不正サイトへのアクセスに起因すると考えられるインシデントの件数が合計で 2,782 件、全体の回答数のうち 83.4%にあたる。

回答者 1,065 名のうち、「フィッシングメールの受信」は 695 名と全回答者数の 65.3%、「ビジネスメール詐欺のメール受信」は 534 名で全回答者の 50.1%と、上位 2 項目では組織の半数以上がメールによるインシデントを経験していることがわかりました。「フィッシングメールの受信」や「ビジネスメール詐欺のメール受信」、「不正サイトへのアクセス」のほか、インシデントの上位に位置する標的型攻撃やランサムウェアの感染なども組織を狙ったメールやフィッシングメール、改ざんサイトの閲覧などがインシデント発生の主な原因となっています。

こうしたインシデントのあった組織でも、リスク管理体制やサイバー事故対応の専門チーム「CSIRT（シーサート）」が概ね機能していると回答した組織は 8 割以上に上り、リスクに対する危機意識は高いことがわかりました。

また、これらの組織は情報セキュリティ対策を「重要課題」と位置付けていますが、さらに重みのある「経営課題」と位置付ける組織は全体の54.6%と、インシデントがあったのにも関わらず全体の約半数に留まっています。

テレワーク導入組織ではテレワーク継続意向 100%、テレワークは恒久化？セキュリティでは出口対策・内部対策を重視

テレワーク導入組織のうち、テレワークを「全社的に導入」しているのは 60%、「大多数が導入」は 23.9%、「一部部署のみ導入」が 16.1%となり、テレワークが広く浸透していることがわかりました。テレワーク導入組織のテレワーク継続意向は、「導入継続予定」が 75.4%、「導入継続見込みだが未定」が 24.6%とテレワーク継続意向は 100%という結果になり、既にテレワークを導入している組織では、テレワークは恒久的に運用していくことが見込まれます。

テレワーク環境では、社内ネットワークや社内ファイルサーバーへの接続が必要となりますが、VPN（仮想私設通信網）やリモートデスクトップ（遠隔地から社内のパソコンを操作）などが多く利用されています。オフィスから持ち出す PC の管理など社内ルールは約 9 割が「徹底」となっていますが、社内ネットワークや社内ファイルサーバーへの接続やセキュリティ対策について、およそ半数が「十分ではない」と回答しています。テレワーク時のセキュリティ対策で重視する領域の上位は、端末やサーバ環境、従業員のセキュリティ教育、ルール作りなどで、概ね「対策済み」となっています。エンドポイント対策としても主要な対策は概ね 5 割以上の組織で網羅されており、重視する領域はアンチウイルスや個人情報（ファイル）、電子メールなどとなっています。

セキュリティ対策として注目される「ゼロトラスト」「SWG」「SASE」の検討が 7 割以上と関心が高い

セキュリティ対策として注目される、すべて信頼しないという考え方からセキュリティ対策を行う「ゼロトラスト」、Web セキュリティ管理機能を統合したクラウドサービス「SWG（セキュアウェブゲートウェイ）」、ネットワークセキュリティ機能と WAN 機能の両方を提供する「SASE（サシ―）」の検討状況を調査したところ、どれも 7 割以上が検討とセキュリティ対策への関心が高いことがわかりました。

ゼロトラストについては、全体の 7 割以上がゼロトラストに基づき対策を検討しています。また、SWG も 8 割以上が検討しており、5,000 人以上の組織では 57.9%と半数以上が SWG を導入済みであることがわかりました。最新のセキュリティフレームワークの一つである SASE も7割以上が検討している状況です。ただ一方で、従業員数 199 人以下の中小企業のうち約5割はゼロトラストや SASE について「意識していない」「わからない」としており、認知や理解が進んでいないことが明らかになりました。

	対策を実施済み	予算取得済み	対策を検討・調査中	検討予定なし	わからない
ゼロトラスト	21.0%	32.2%	23.3%	17.7%	5.8%
SWG	42.7%	25.4%	19.8%	6.9%	5.1%
SASE	21.6%	22.1%	28.9%	15.7%	11.7%

組織規模に関わらず外部攻撃によるインシデントが発生　入り口となる Web アクセスとメールの対策がますます重要に

今回の調査結果より、テレワーク導入組織が 2020 年に経験したインシデントは Web アクセスとメールに起因する外部攻撃であり、組織規模に関わらずインシデントに遭遇していることがわかりました。これらの組織はセキュリティ対策を重要課題と位置づけ、ゼロトラストなど従来の境界型に依存しないセキュリティモデルの対策も重視するなど決して対策を疎かにしているわけではありません。ただし、多くの組織が重要視するのは、従業員の持ち出し端末やセキュリティルールの構築、従業員のセキュリティ教育といった人的資源の対策の優先度が高いのも事実です。

メールや Web アクセスに起因するインシデントがほとんどであるのに対して、これらの対策よりも端末や人的資源の対策が優先される理由は、サイバー攻撃が巧妙化したことによりシステムによる入口対策が困難とされ、侵入された際の内部対策や出口対策が重視されるようになったためと考えられます。しかし、今回判明したように、侵入経路は依然として Web アクセスとメールがほとんどです。

今回調査したテレワーク導入組織では、セキュリティの脅威を認識しつつもテレワークを前向きに継続していく姿勢が伺えました。アフターコロナの日本では、テレワークを基本の働き方とするなど今後の働き方はさらに多様化します。働き方が多様化する中で端末管理や従業員のモラルといった人的資源の対策だけでは限界があり、多くのインシデントの原因となっている Web アクセスとメールを使った主要な攻撃手法に合わせた入口対策を実施していくことが改めて重要になります。

デジタルアーツでは定期的に行う情報セキュリティに関する調査を通じて、企業・官公庁をターゲットとするインシデントが増加している傾向から、経営の根幹を揺るがしかねない情報漏洩を防止するための注意喚起をし続けることで、インシデントの減少に寄与してまいる所存です。引き続き、情報セキュリティメーカーとして全国レベルの調査結果を通じてさまざまな情報を提供してまいります。

調査概要	
調査対象	全国の民間企業や官公庁の情報セキュリティ担当者 ・自組織のセキュリティインシデント状況を把握し、情報セキュリティ対策の意思決定に関わり ・2020 年に何らかのセキュリティインシデントを経験した組織に限る
調査機関	2021 年 4 月 16 日（金）～4 月 21 日（水）
調査方法	インターネット調査
有効回答数	1,065 サンプル
実施期間	クロス・マーケティング

デジタルアーツ株式会社　概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、有害情報の閲覧を制限する Web フィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア　ウエストタワー14F
URL: https://www.daj.jp/

＜本リリースに関するお問い合わせ＞
デジタルアーツ株式会社　広報担当　山田
※新型コロナウイルス感染症拡大に伴う在宅勤務実施中のため、お電話でのお問い合わせは以下とさせていただきます
TEL　：090-1555-7254　/ E-mail : press@daj.co.jp

より便利な、より快適な、より安全なインターネットライフに貢献していく