

報道関係者各位

～攻撃発覚まで“90日”を超えた事案が増加、全体の6割以上に！～
サイバー攻撃の発生から発覚・公表までの日数に関する調査レポート【2021年版】を発表

株式会社サイバーセキュリティクラウド(本社:東京都渋谷区、代表取締役社長 兼 CEO:小池敏弘、以下「当社」)は、2020年9月1日から2021年8月31日までに公表された法人・団体における不正アクセスに関する個人情報漏洩数1,000件以上の主な個人情報流出事案に基づき、サイバー攻撃の発生から発覚・公表までの期間に関する調査レポートを発表いたします。

■攻撃発覚までやや短期化するも、依然として1年近く気付かれないままに



2020年9月1日から2021年8月31日の期間内で公表された、国内法人や団体における個人情報漏洩数1,000件以上の事案を対象に調査を実施(以下「2021年調査」とする)。調査では法人や団体がサイバー攻撃を受けた攻撃の「発生日」から、攻撃に気づいた「発覚日」までに平均349日を要していることがわかりました。これは当社が2020年8月に実施した、2019年1月から2020年7月までを対象期間とした「サイバー攻撃の発生から発覚・公表までの期間に関する調査」(以下「2020年調査」とする)における「発生日」から「発覚日」までの平均日数と比較すると34日短期化しています。

また「発覚日」から被害が公表された「公表日」までには平均82日を要しており、2020年調査と比較すると13日短くなっています。攻撃の発生から発覚までやや短期化したものの、依然として法人や団体は1年近くもの間、サイバー攻撃の被害に気付いておらず、さらに発覚から公表するまでにかかった時間が増加していることがわかりました。

■攻撃発覚まで“90日”を超えた事案が6割超え、2020年調査よりも10ポイント増加

調査対象期間中の事案を「発生」から「発覚」までに要した期間を「30日以内」、「30日超90日以内」、「90日超180日以内」、「180日超1年以内」に分類した場合、発生してから発覚するまでに“90日超”を要した事案が、全体の6割を超えました。これは2020年調査時(90日超:51.7%)と比較して10ポイント近く増加しています。また「30日以内」が11.9ポイント減少し、「1年超」が7.7ポイント増加しています(表1)。発見までに時間がかかっている要因の一つとして、新型コロナ禍でオンライン化が進む中、企業が攻撃を発見する仕組みが整備されていないことや、定期的なセキュリティチェック体制を構築できていないことが考えられます。

表1: 攻撃発生から発覚までの日数

	2021年調査	2020年調査	増減
30日以内	29.5%	41.4%	-11.9
30日超90日以内	9.1%	6.9%	+2.2
90日超180日以内	11.4%	12.1%	-0.7
180日超1年以内	18.2%	15.5%	+2.7
1年超	31.8%	24.1%	+7.7

■被害に気付いて公表するまで“90日”を超える事案が増加

「発覚日」から「公表日」までを分類した場合、発覚してから公表するまでに“90日超”を要した事案が全体の34.3%を占め、2020年調査と比較して3.5ポイント増加しました(表2)。公表までに被害の原因や影響範囲の特定、利害関係者への通知・説明が求められる中、企業側の人的リソースが不十分だったり、コミュニケーションや連携がうまく取れていないことで公表までの時間が長期化していると考えられます。また、2022年4月までに全面施行される改正個人情報保護法では、本人への通知や個人情報保護委員会への報告の義務化など事業者の責務が追加されるため、公表にかかる時間がさらに増えることも予想されます。

表2: 攻撃発覚から公表までの日数

	2021年調査	2020年調査	増減
30日以内	48.5%	50.6%	-2.1
30日超90日以内	17.1%	18.5%	-1.4
90日超180日以内	22.9%	18.5%	+4.4
180日超1年以内	8.5%	11.1%	-2.6
1年超	2.9%	1.2%	+1.7

■サイバーセキュリティクラウド 代表取締役 CTO 渡辺洋司のコメント

今回の調査では攻撃から発覚まで1年超を要したものが全体の約3割を占めるなど、発覚まで長期を要した事案の割合が増加していました。企業のデジタル化が進むとともに、サイバー攻撃の被害に遭う機会が増加しており、また、サイバー攻撃は年々高度かつ多様になっています。そのため攻撃の発生後、長期間を経てようやく被害に気づく事案が増加傾向にあると考えられます。さらに一度攻撃を許してしまうと、被害に遭うまでその状況に気づくのは困難です。こうした事態を未然に防ぐためには、サイバー攻撃の被害を対岸の火事と捉えず、定期的に自社のWebサイトの脆弱性を確認したり、攻撃を未然に防ぐことが可能な仕組みづくりや、素早く攻撃に気付けるような社内体制の構築が一層重要になっていくと考えられます。

<調査概要>

-調査対象期間:2020年9月1日~2021年8月31日

-調査対象:上記期間までに公表された法人・団体における不正アクセスに関する被害規模1千件以上の主な個人情報流出事案(87件)

-調査方法:サイバーセキュリティクラウド調べ

【株式会社サイバーセキュリティクラウドについて】

会社名:株式会社サイバーセキュリティクラウド

所在地:〒150-0011 東京都渋谷区東 3-9-19 VORT 恵比寿 maxim3 階

代表者:代表取締役社長 兼 CEO 小池 敏弘

設立:2010年8月

URL:<https://www.cscloud.co.jp/>

<本件のお問い合わせ>

株式会社サイバーセキュリティクラウド経営企画部

広報担当:竹谷

電話:03-6416-9996 FAX:03-6416-9997

E-mail:pr@cscloud.co.jp

サイバーセキュリティクラウド PR 事務局(スキュー内)担当:北出・金子

TEL:03-6450-5457 E-Mail:csc@skewinc.co.jp