【ニュースリリース】

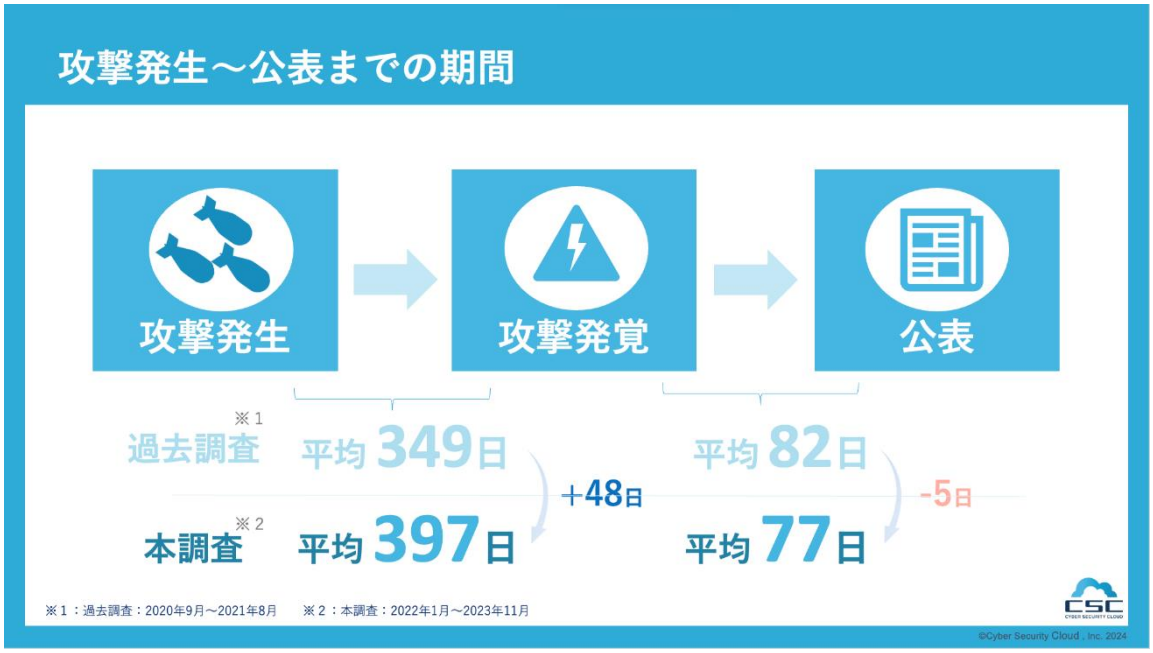
2024 年 2 月 21 日
株式会社サイバーセキュリティクラウド

報道関係者各位

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
多くの企業が気づいていない？
1,000 件以上の個人情報を流出した法人・団体で
サイバー攻撃発生から攻撃発覚までにかかる期間は 1 年以上！

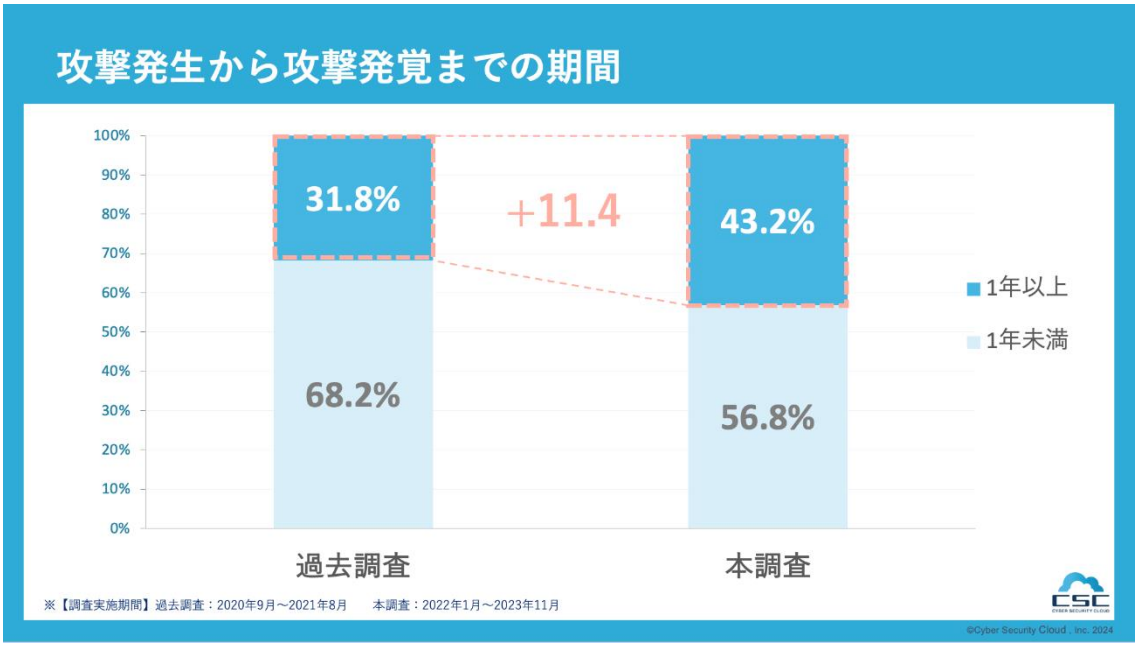
ハッカー対策サービスを展開するグローバルセキュリティメーカーの株式会社サイバーセキュリティクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池 敏弘、以下「当社」）は、2022 年 1 月 1 日から 2023 年 11 月 30 日までに公表された不正アクセスに関する個人情報流出事案（個人情報漏洩数 1,000 件以上）に基づき、サイバー攻撃の発生から発覚・公表までの期間に関する調査レポート（以下「本調査」）を発表いたします。

■攻撃発覚から公表までの期間については多少短期化するも、攻撃発生から攻撃発覚までは 1 年近く気付かれないままに



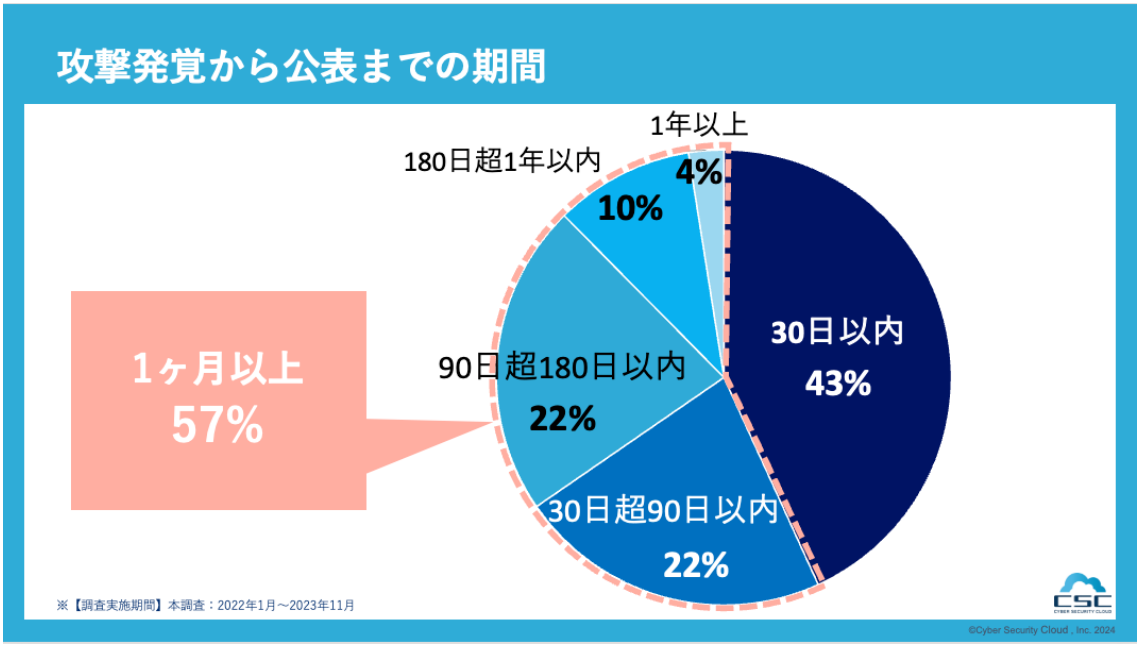
本調査では、法人や団体がサイバー攻撃を受けた攻撃の「攻撃発生」から、攻撃に気づいた「攻撃発覚」までに平均 397 日を要していることがわかりました。これは当社が過去（2020 年 9 月から 2021 年 8 月までを対象期間）に実施した調査（以下「過去調査」）の「攻撃発生」から「攻撃発覚」までの平均日数と比較すると、48 日長期化しています。
また「攻撃発覚」から被害が公表された「公表」までには、本調査で平均 77 日を要しており、過去調査と比較すると 5 日短くなっています。
「攻撃発生」から「攻撃発覚」までは長期化する結果となり、1 年以上もの間サイバー攻撃の被害に気付いていない状況にあることがわかりました。また「攻撃発覚」から「公表」するまでにかかった時間はやや短期化したものの、「公表」までには 2 か月以上の時間がかかることがわかりました。

■「攻撃発生」から「攻撃発覚」まで 1 年以上の事案が約 4 割、過去調査よりも 11.4%増加



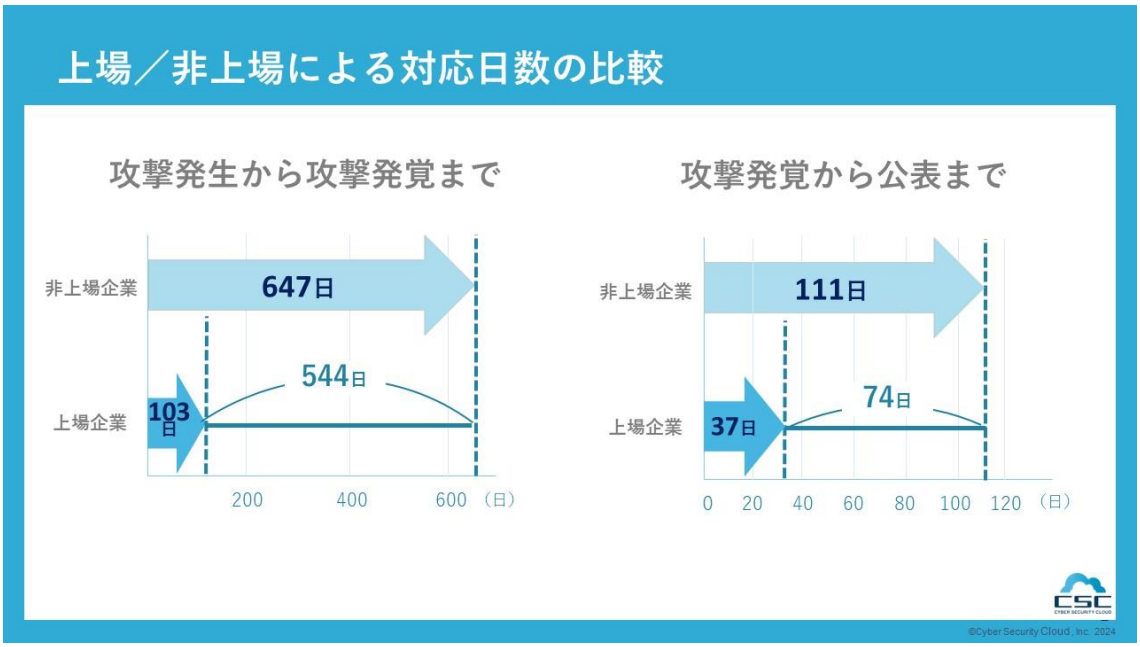
「攻撃発生」から「攻撃発覚」までに要した期間を「1 年未満」と「1 年以上」に分類した場合、「1 年未満」は 56.8%という結果となりました。一方、「1 年以上」は 43.2%と、過去調査より 11.4%増加。「攻撃発覚」までに 1 年以上かかった要因の一つとして、未知の脆弱性（Zero-Day）を利用した攻撃により、その脆弱性が公に知られるまで検出されないことが挙げられます。さらに、Web アプリケーションは絶えず変化しており、新機能やアップデートが頻繁に行われるため、Web アプリケーションの更新及び監視に割くリソースやコストなどの問題から、脆弱性が長期間にわたって放置されるケースもあります。

■「攻撃発覚」から「公表」まで 1 ヶ月以上かかっている事案は 57%



【本件に関するお問い合わせ】
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・川﨑
TEL：03-6416-9996 携帯:080-4583-2871(川﨑携帯)FAX：03-6416-9997
E-Mail：pr@cscloud.co.jp

「攻撃発覚」から「公表」までの期間を分類した結果、1 ヶ月以上かかっている事案は 57%となりました。この長期化の背景には、複数の要因が考えられます。公表までに被害の原因や影響範囲の特定、影響を受ける利害関係者への適切な通知・説明が求められる中、企業側の人材が不十分だったり、攻撃発覚から公表までのプロセスに関する明確なレギュレーションが設けられていないことなど、様々な要因により公表までの時間が長期化していると考えられます。



「攻撃発生」から「攻撃発覚」までに要する期間について上場企業と非上場企業で比較したところ、上場企業が平均 103 日だったのに対し、非上場企業は平均 647 日となりました。また「攻撃発覚」から「公表」までに要する期間は上場企業が 37 日だったのに対し、非上場企業は 111 日となりました。上場企業の方が非上場企業に比べて、サイバー攻撃に対してより早く対応していることがわかります。コンプライアンスの遵守やステークホルダーへの影響を重視し、迅速な対応を上場企業が求められていることは、この差の一つの要因だと考えられます。

■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

本調査では、「攻撃発生」から「攻撃発覚」するまでの期間が平均で 397 日という結果となりました。これは、攻撃者が長期間にわたってシステム内に潜伏し、企業の貴重なデータにアクセスし続けることを可能にしています。このような状況は、特に中小企業において顕著です。サイバーセキュリティ人材の不足やリソースの限られている中小企業は、攻撃を発見し対応するまでにより多くの時間を必要としています。一方で、「攻撃発覚」から「公表」までの期間がやや短期化している点は、セキュリティ意識の高まりと対応スピードの向上を示唆しています。特に上場企業では、サイバーセキュリティへの意識が非上場企業に比べて高く、迅速な対応傾向が見られます。しかし、「公表」までに 2 か月以上の時間を要しているのは、どのようなデータが漏洩したのか、攻撃者がアクセスしたシステムは何か、などを確認するための詳細な調査と分析を行い、正確な情報を集めるために時間がかかることがあります。また、多くの場合、サイバー攻撃の詳細は公開されておらず数年後に発覚することも多々あります。
サイバーセキュリティは、企業にとって不可欠な要素です。これらの調査結果を踏まえ、企業は、最新の技術と継続的な教育を通じて、サイバーセキュリティの体制を強化し続ける必要があります。

【本件に関するお問い合わせ】
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・川﨑
TEL：03-6416-9996 携帯:080-4583-2871(川﨑携帯)FAX：03-6416-9997
E-Mail：pr@cscloud.co.jp

＜調査概要＞
-調査対象期間：2022 年 1 月 1 日～2023 年 11 月 30 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（92 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
住所　　：　東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 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
サイバーセキュリティクラウドは「世界中の人々が安心安全に使えるサイバー空間を創造する」という経営理念を掲げ、世界有数のサイバー脅威インテリジェンスと AI 技術を活用した、Web アプリケーションのセキュリティサービス、及び脆弱性情報収集・管理ツールといったハッカー対策サービスを提供しています。これからも私たちは WAF を中心としたサイバーセキュリティにおけるグローバルリーディングカンパニーの 1 つとして、情報革命の推進に貢献してまいります。

【本件に関するお問い合わせ】
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・川﨑
TEL：03-6416-9996 携帯:080-4583-2871(川﨑携帯)FAX：03-6416-9997
E-Mail：pr@cscloud.co.jp