

NEWS RELEASE

2026 年 10 月 29 日

株式会社ブロードバンドセキュリティ

国内で相次ぐ不正アクセスを受け、BBSec が 「見えないセキュリティリスク」の可視化と対策強化を提言

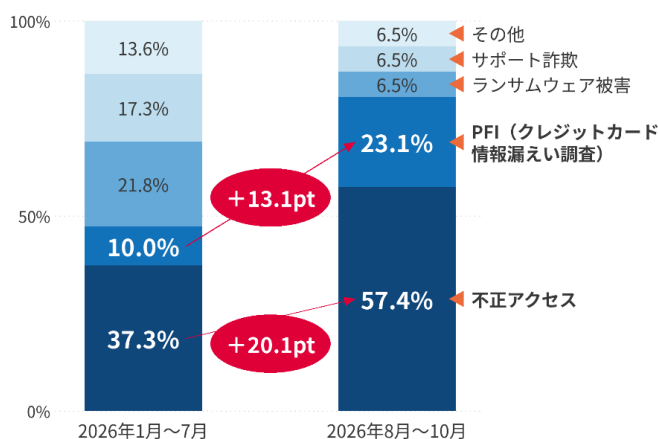
～公開 IT 資産・情報漏えいの兆候の把握から、脆弱性の改善、継続的な監視・対応まで～

情報漏えい IT 対策などセキュリティに特化したサービスを提供する株式会社ブロードバンドセキュリティ（本社：東京都新宿区、代表取締役社長：森澤 正人、以下 BBSec）は、国内で相次ぐ不正アクセスによる被害の公表を受け、企業・団体に対し、外部から見た自組織の公開資産と情報漏えいの兆候を把握し、その結果に基づいて対策を進めることを提言します。

主な対象は、小売・EC、旅行・宿泊、交通、金融など会員・顧客情報を扱うサービスを運営する企業や、製造・物流など、関係会社・拠点・委託先にまたがるシステムを利用する企業です。事業責任者と IT・セキュリティ責任者が連携し、現在のリスクと事業への影響を把握したうえで、優先して取り組むべき対策を判断することと呼びかけます。

■相次ぐ不正アクセスを踏まえ、まず自社の現状を把握する

BBSec に寄せられたセキュリティインシデントに関するお問い合わせでは、不正アクセスに関する相談の割合が、2026 年 1 月～7 月の 37.3%から 8 月以降は 57.4%へ上昇しています。



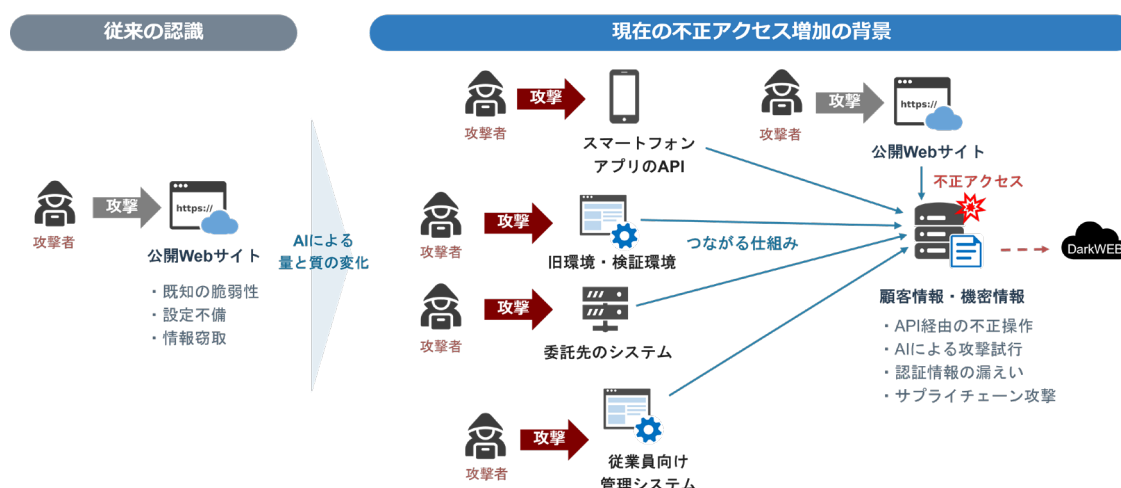
1～7月：前回資料の構成比／8～10月：今回集計（10/27まで、PFI疑い含む）

JPCERT/CC は、国内組織で相次ぐ不正アクセスに関する注意喚起において、侵害原因や攻撃手法を整理しており、既知の脆弱性や管理不備を狙った攻撃、API 経由の不正操作、BI ツール・従業員向け管理システムからの情報漏えいなどを列挙しています。また、2026 年 10 月 23 日の更新では、AI を用いたペネトレーションテスト基盤を悪用した攻撃試行も追加しています※1。

BB5ec は 2026 年 10 月 8 日に、公開 Web サービスの基本対策の再点検を提言しました※2。今回は、その点検を具体的な行動につなげるため、まず「攻撃者から自社のシステムがどう見えているか」「自社に関する情報が外部に流出していないか」を確認することを提言します。

自社で把握しているシステムだけを対象に点検していると、旧環境や検証環境、関係会社・委託先が管理するシステムなどが対象から漏れる可能性があります。また、情報漏えいは、サービス停止などの目に見える異常を伴わず既に発生している場合もあります。

公開Webサイトだけでなく、つながる仕組みも攻撃対象となっている



そのため、社内の管理情報に加え、外部から確認できる公開資産や情報の流通状況を調査し、対策の抜け漏れや、調査・対応を急ぐべき兆候がないかを把握することが重要です。

■業界・業務に応じて確認する対象と役割を明確にする

小売・EC、旅行・宿泊、交通などのサービス運営企業では、会員登録、予約、購入、ポイント利用などの機能と、それらが扱う顧客情報を確認対象とします。事業責任者やサービス運営責任者は、IT・セキュリティ責任者とともに、Web サイト、スマートフォンアプリ、API、管理機能、委託運営環境まで点検範囲に含まれているかを確認します。

金融・決済などの企業では、システムリスク管理部門や IT・セキュリティ部門が中心となり、重要な顧客情報へのアクセス経路、認証情報・API キーの管理、不正な権限変更や情報の大量取得を把握できるかを確認します。

製造・物流など、関係会社・拠点・委託先が多い企業では、情報システム責任者やグループ IT 統括部門が、業務システムやポータル、遠隔保守環境などの公開状況と管理責任を確認します。

経営層・事業責任者には、調査結果を踏まえて改善の優先順位と対応責任者を定め、必要な対策を実行できる体制を整えることを呼びかけます。

■企業・団体に提言する三つの取り組み

1. 公開資産と情報漏えいの兆候を把握する

アタックサーフェス管理（ASM：Attack Surface Management）の取り組みとして、インターネットから確認できる自組織の IT 資産を調査し、把握できていなかったシステム、管理画面、不要な公開、脆弱性が疑われる箇所などを確認します。

あわせて、ダークウェブ等で、自社に関連する認証情報や顧客情報、機密情報が公開・流通していないかを調査します。漏えいした認証情報は、さらなる不正アクセスの足がかりとなるおそれがあるため、発見した情報の内容に応じて、認証情報の無効化やアクセス履歴の調査などにつなげます。

2. Web・API などの問題を詳しく調べ、改善する

現状把握の結果と事業への影響を踏まえ、優先すべきシステムを特定し、脆弱性や設定不備を詳しく確認します。

顧客向けの Web 画面だけでなく、スマートフォンアプリが利用する API や管理機能についても、認証・権限制御が適切か、他の利用者の情報を取得できないか、権限のない操作を実行できないかを点検します。発見した問題は、対応責任者と期限を定めて修正し、修正後の再確認や、機能追加・構成変更に応じた点検につなげます。

3. 侵入を前提に、早期発見と被害拡大を抑える対応を整える

脆弱性の修正や設定の適正化とあわせて、侵入された場合にいかに早く異常を発見し、被害拡大を抑えられるかを確認します。

端末、認証基盤、ネットワークなどの監視対象と必要なログを整理し、検知後に分析・判断する担当者、夜間・休日の連絡先、端末隔離やアクセス遮断などの対応手順を明確にします。

これらは、お客様の対策状況とリスクに応じて組み合わせて進める取り組みです。侵害の兆候が確認された場合は、他の点検や診断の完了を待たず、被害の調査と拡大防止への対応を優先します。

■BBSecによる支援

BBSecは、アタックサーフェス調査とダークウェブ調査による現状把握から、Web・APIの脆弱性診断、G-MDRによる継続的な監視・分析と対応支援までを通じて、情報資産の保護と事業継続を支援します。

1. 公開資産と情報漏えいの兆候を把握するための支援

BBSecは、アタックサーフェス調査サービスとサイバー脅威情報調査サービスを通じて、外部から見たリスクと漏えいの兆候を把握し、対応の要否や優先順位の判断を支援します。ダークウェブ等の継続的な調査により、その後の情報の公開・流通状況の変化の把握も支援します。

2. Web・APIなどの問題を把握し、改善するための支援

BBSecは、Webアプリケーション・APIの脆弱性診断やクラウド設定診断などを通じて、問題の把握と改善、修正後の再確認を支援します。

3. 侵入や異常の早期発見と、被害拡大を抑えるための支援

BBSecは、G-MDRによる継続的な監視と複数のログを組み合わせた相関分析を通じて、不審な挙動の検知、原因・影響範囲の分析、封じ込めに向けた対応を支援します。あわせて、CSIRT体制や対応手順の整備を支援し、検知を具体的な行動につなげます。

【ご相談とお問い合わせ】

当社では、不正アクセスや情報漏えいなどのセキュリティ事故が発生した場合や、その疑いがある場合に備え、サイバーインシデント緊急対応ご相談窓口を設けています。

サイバーインシデント緊急対応ご相談窓口：

<https://cr.bbsec.co.jp/cyberincident119>

フリーダイヤル：0120-085-490

その他、サイバーセキュリティ対策状況の点検や改善の優先順位のご相談については、当社営業担当または当社Webサイトからお問い合わせください。

<https://www.bbsec.co.jp/>

【BBSec について】

BBSec は、2000 年創業のトータルセキュリティ・サービスプロバイダーです。現状の可視化や診断から事故発生時の対応、24 時間/365 日体制での運用まで、フルラインアップのサービスを提供しています。高い技術力と豊富な経験、幅広い情報収集力を生かし、「サプライチェーンを狙った攻撃」「社会インフラを狙った攻撃」「AI 時代のセキュリティ」を解決すべき社会課題ととらえ、より多くのお客様を悪意ある攻撃者から守ることで、「便利で安全なネットワーク社会を創造する」というビジョンを実現します。

【本リリースに関するお問い合わせ】

株式会社ブロードバンドセキュリティ 経営企画部

TEL : 03-5338-7430 E-mail : press@bbsec.co.jp

【参考資料】

※1 JPCERT/CC／「直近で相次いでいる国内組織における不正アクセスに関する注意喚起」

／2026 年 10 月 23 日更新

<https://www.jpcert.or.jp/at/2026/at260030.html>

※2 BBSec／「国内で相次ぐ不正アクセスを受け、BBSec が公開 Web サービスの基本対策の再点検を提言」

／2026 年 10 月 8 日

<https://www.bbsec.co.jp/news/20261008.html>

以上