



2026年10月8日

各 位

会 社 名 株式会社ブロードバンドセキュリティ
代 表 者 名 代表取締役社長 森澤 正人
(コード 4398 東証スタンダード)
問 合 せ 先 管理本部経営企画部長 高田 宜史
(TEL 03-5338-7430)

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

～AI 時代に警戒すべきは、脆弱性や設定不備を狙う攻撃の「量」と「速度」の変化～

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、インターネットに公開された Web サービスを運営する企業・団体に対し、基本的なセキュリティ対策の再点検を提言します。

BBSec は、AI 時代に企業・団体がまず警戒すべきは、特殊な新しいサイバー攻撃よりむしろ、脆弱性や設定不備を狙う従来型の攻撃の「量」と「速度」の変化であると考えます。この見解に基づき、Web アプリケーション、システム間の連携に使う API、コンテンツ管理システム（CMS）、管理者用画面などを対象に、脆弱性の修正、設定の適正化、認証・権限管理を徹底し、対策の実効性を継続的に確認することと呼びかけます。

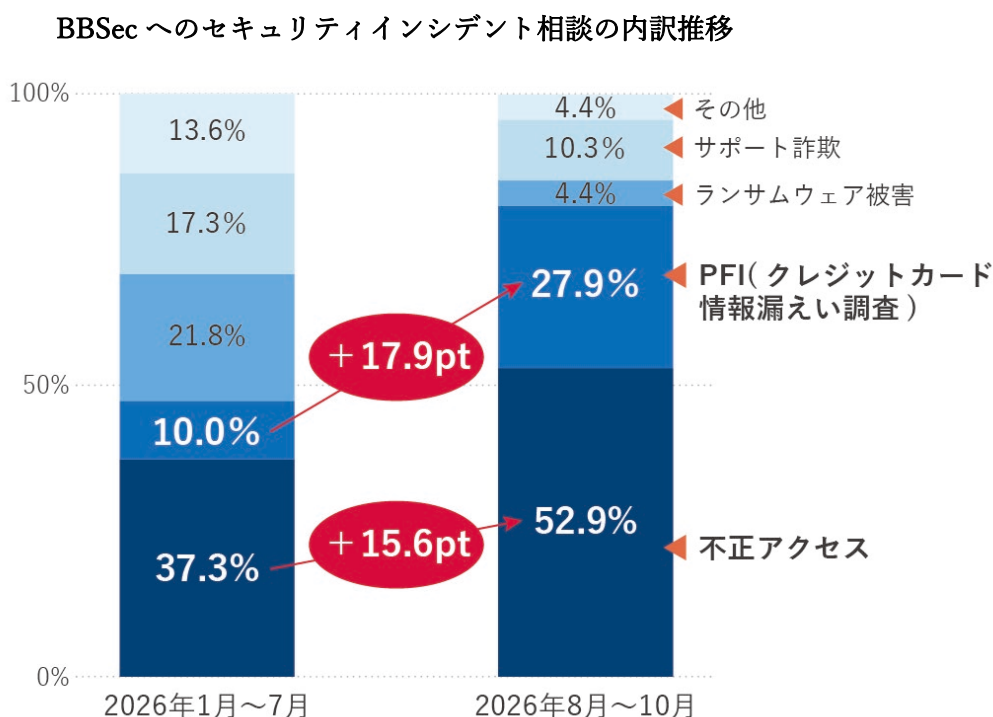
■AI 時代に警戒すべきは、脆弱性や設定不備がより多く・より速く狙われること

「AI を使った攻撃」と聞くと、これまでの対策が通用しない特殊な攻撃を思い浮かべるかもしれません。しかし、BBSec が企業・団体にまず警戒を促したいのは、従来から対策が求められてきた脆弱性や設定不備を狙う攻撃が、AI によって、より多く・より速く行われるようになることです。

攻撃者が AI を活用することにより、攻撃対象システムの調査や脆弱性の発見が効率化され、より多くの対象を、より短時間で狙えるようになると考えられます。つまり、BBSec は、企業・団体にとって身近な脅威は、「知らない手口で攻撃されること」よりむしろ、「未修正の脆弱性や設定不備を、対処する前に突かれること」にあると考えます。

英国国家サイバーセキュリティセンター（NCSC）も、2027 年に向けて、新たな攻撃経路の創出よりも、既存の攻撃手法の進化・強化を通じて、AI が侵入の量と影響を増大させると予測しています。また、既知の脆弱性が公表されてから悪用されるまでの時間も、さらに短縮するとしています※1。

実際、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も、不正アクセスに関する相談の割合が、2026 年 1～7 月の 37.3%から 8 月以降は 52.9%へ上昇しています。



※2026 年 10 月 7 日までの集計

■だからこそ、公開 Web サービスの基本対策を再点検する

公開 Web サービスでは、Web アプリケーションの脆弱性、設定不備、認証・アクセス制御の不備など、従来から対処が求められてきた問題への備えが引き続き重要です。独立行政法人情報処理推進機構（IPA）も「安全なウェブサイトの作り方」において、こうした脆弱性への対策と、Web サイトの安全性を高める運用上の取り組みを示しています※2。

BBSec は、AI 時代の備えとして、まず基本対策の徹底を優先すべきと考えます。攻撃者が脆弱性や設定不備を見つけて悪用するまでの時間が短くなるからこそ、防御側も問題の把握から修正・再確認までを滞りなく進める必要があります。

過去に脆弱性診断やセキュリティ対策を実施した Web サービスでも、その後に追加された API、更新された CMS、管理者用画面、関連するクラウド環境などに、対策の抜け漏れが生じていないかを確認することが必要です。「以前に診断した」「対策製品を導入した」という状態で止めず、現在の公開範囲と構成に合わせて、対策の実効性を見直すことを提言します。

あわせて、不審なアクセスを早期に把握し、被害拡大を防ぐ対応も重要です。BBSec は、公開資産の把握、脆弱性の診断と改善、継続的な監視、セキュリティ事故（インシデント）対応を通じて、公開 Web サービスの安全性と事業継続を支援します。

■企業・団体に推奨する三つの点検

1. 侵入の入口を減らす

－公開しているシステムと、認証・権限の管理状況を確認します－

Web サイト、API、CMS、遠隔接続に使う VPN 機器、クラウド環境などに加え、旧環境・検証環境や外部連携先も把握し、不要な公開、未修正の脆弱性、設定不備を確認します。診断済みのシステムについても、機能追加や構成変更が診断範囲に反映されているか、指摘事項が修正されているかを確認します。

管理者・保守アカウントの多要素認証、不要アカウントの削除、権限の最小化、API への接続に使う認証情報（API キー等）の管理を点検します。決済や会員情報の変更などの機能では、他の利用者の情報への不正なアクセスや、権限のない操作を防げるかも確認します。

2. 侵入や異常を早く見つける

－異常を検知できるかに加え、検知後に対応できるかを確認します－

不審なログイン、強い権限を持つアカウント（特権アカウント）の不正な作成、権限変更、情報の大量取得などを把握するため、必要なログ（システムの動作やアクセスの記録）の取得・保管、監視対象の抜け漏れ、検知後に分析・判断する担当者に対応手順を確認し、夜間・休日でも対応できる体制を整えます。

広告タグ、アクセス解析タグ、外部サービスを利用した問い合わせフォーム、動画・SNS 連携などの外部スクリプト（外部サービスが提供するプログラム）は、利用目的、管理担当者、読み込むスクリプトと通信先を把握します。外部サービスの変更や改ざんによる想定外の通信は、自社サーバーの監視だけでは把握できない場合があるため、利用者のブラウザで発生する通信も確認します。

3. 被害の拡大を抑え、復旧につなげる

－被害発生時の判断・連絡体制と、調査・復旧の手順を確認します－

端末の隔離やサービス停止の判断者、調査に必要なログ等の証拠保全手順、委託先・関係部門との連絡方法を明確にします。バックアップが不正な削除や暗号化の影響を受けにくい形で保管され、実際に復元できるかを確認し、初動から調査・復旧までの手順を訓練等で検証します。

侵入が疑われる場合は、脆弱性の修正に加え、過去の侵入の痕跡や被害範囲を調査します。ダークウェブ※3等の調査は、漏えい情報の外部公開状況を把握する補助手段となります。

■BBSec による支援

BBSec は、Web サービスのみならず企業・団体全体で対策に抜け漏れがないかを確認し、リスクと業務への影響に応じて、優先して改善すべき事項の整理を支援します。

1. 侵入の入口を減らすための支援

インターネットに公開されているシステムを調査し、把握できていなかった公開資産や、攻撃の入口となる脆弱性や設定不備を確認します。公開資産の調査、Web サービスの脆弱性の診断、クラウドの設定診断などで、問題の把握と改善を支援します。

2. 侵入や異常を早く見つけるための支援

システムのログなどを監視して不審なアクセスを検知し、原因や影響範囲の分析から、被害拡大を防ぐための対処までを支援します。また、Web サイトで利用する広告やアクセス解析などの外部スクリプトの通信先を監視し、危険なサイトへの誘導や情報漏えいにつながる不審な通信の把握を支援します。

3. 被害の把握と復旧に向けた支援

被害発生時の対応体制や対応手順の整備、被害の原因や範囲を明らかにするための調査、復旧・再発防止に向けた対応を支援します。また、ダークウェブ調査により、被害が判明した際の漏えい情報の外部公開状況の把握に加え、まだ認識されていない情報漏えいの兆候の把握を支援します。特に、公開 Web サービスでは、情報漏えいがサービス停止などの目に見える異常を伴わない場合もあり、外部での情報の公開・流通状況が、被害に気づく手がかりとなります。

各支援の対象範囲や提供条件は、お客様の環境やご要望を確認したうえで個別にご案内します。

BBSec は、リスクの把握や対策の導入から継続的な監視・運用、有事の対応までをつなぐことで、企業・団体の情報資産の保護、サービス利用者の安全確保、事業継続を支援してまいります。

【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】 2026 年 10 月 7 日確認

※1 英国国家サイバーセキュリティセンター（NCSC）／「Impact of AI on cyber threat from now to 2027」／2025 年 5 月
7 日

<https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027>

※2 独立行政法人情報処理推進機構（IPA）／「安全なウェブサイトの作り方」

<https://www.ipa.go.jp/security/vuln/websecurity/about.html>

※3 ダークウェブ：専用のソフトウェア等でアクセスする、通常の検索エンジンでは検索できないインターネット上の領域。漏えい情報の公開・売買に利用されることがあります。

以上