かつてない脆弱性数の増加に どう立ち向かうべきか

～ランチのおともにDNS～

2026年11月26日

Internet Week 2026 ランチタイムセミナー

株式会社日本レジストリサービス（JPRS）

森下 泰宏・熊谷 維魅

Copyright © 2026 株式会社日本レジストリサービス

講師自己紹介

- 森下 泰宏（もりした やすひろ）
  - 所属：JPRS 技術広報担当・技術研修センター
  - 主な業務内容：技術広報活動全般・社内外の人材育成
  - 一言：**17回目の登壇です！JPRSランチセミナーは20回目です！**



- 熊谷 維魅（くまがい いみ） Internet Week 2026 プログラム委員
  - 所属：JPRS システム部・技術研修センター
  - 主な業務内容：ネットワークの構築運用・DNS関連イベントの講師など
  - 一言：**3年連続3回目の登壇です！更にわかりやすい説明を心がけます！**

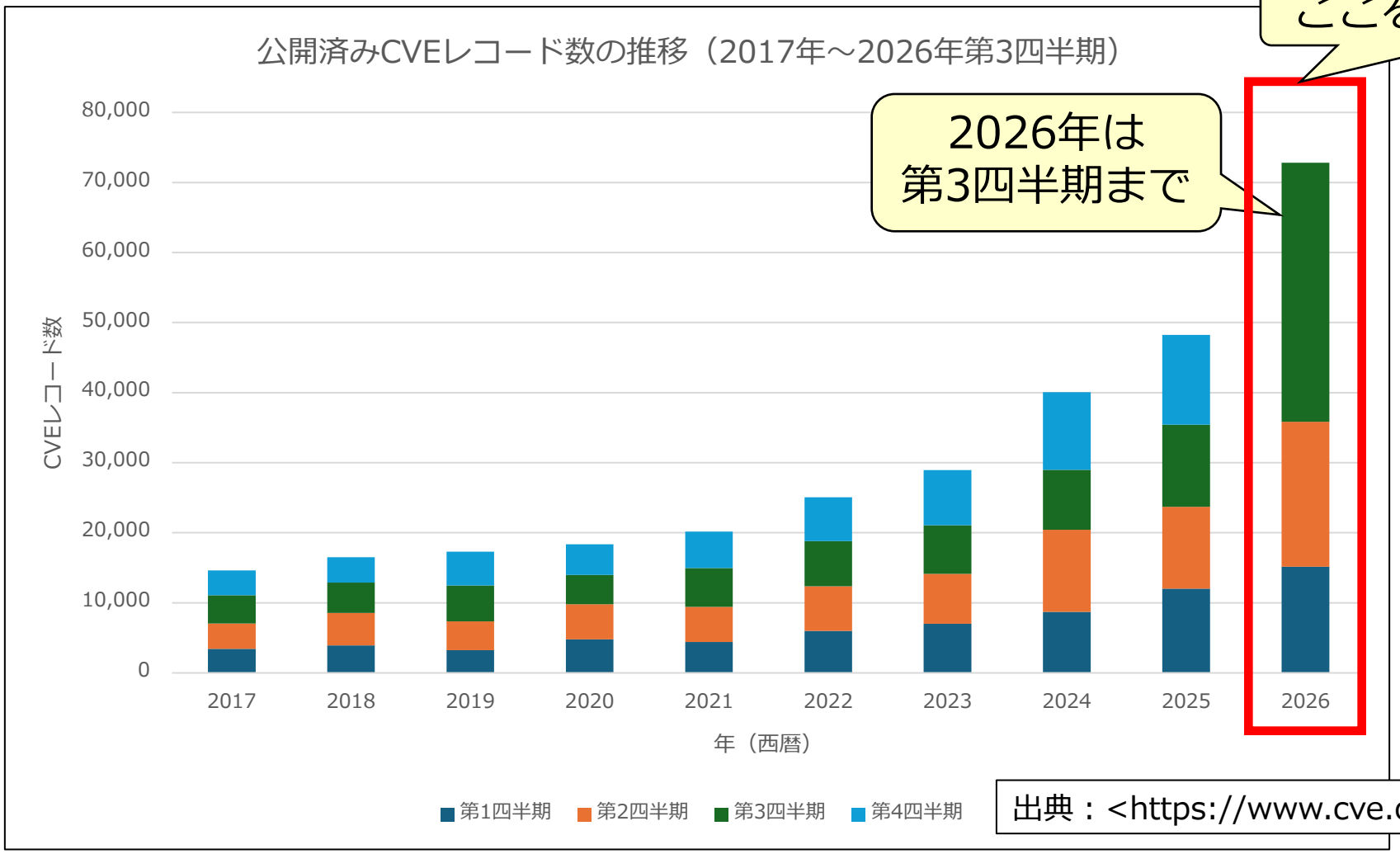


Copyright © 2026 株式会社日本レジストリサービス

はじめに：脆弱性の数は どの程度増えているのか？

Copyright © 2026 株式会社日本レジストリサービス

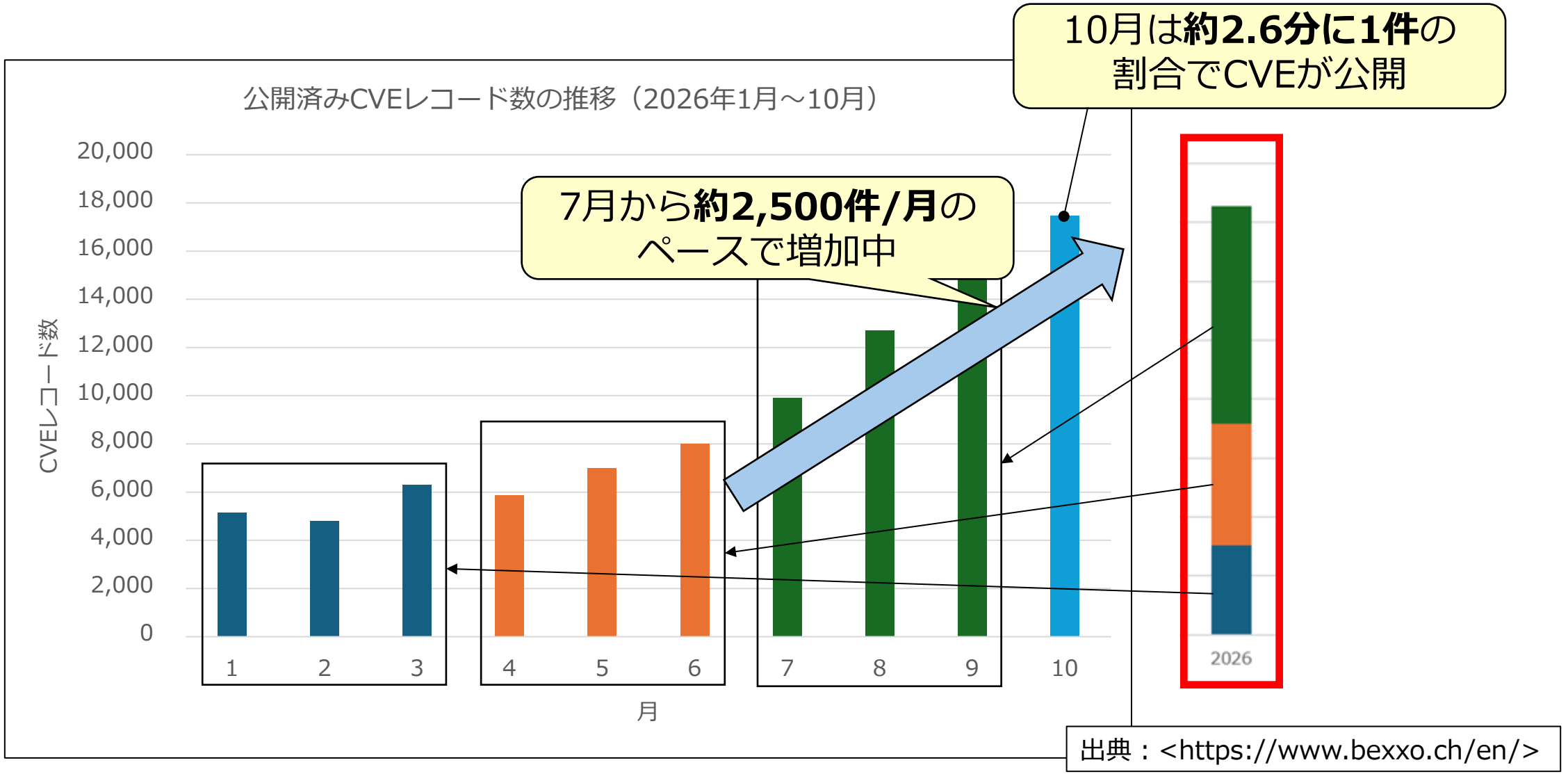
公開済みCVEレコード数の推移（2017年～）



出典：<https://www.cve.org/about/Metrics>

Copyright © 2026 株式会社日本レジストリサービス

公開済みCVEレコード数の推移（1月～10月）

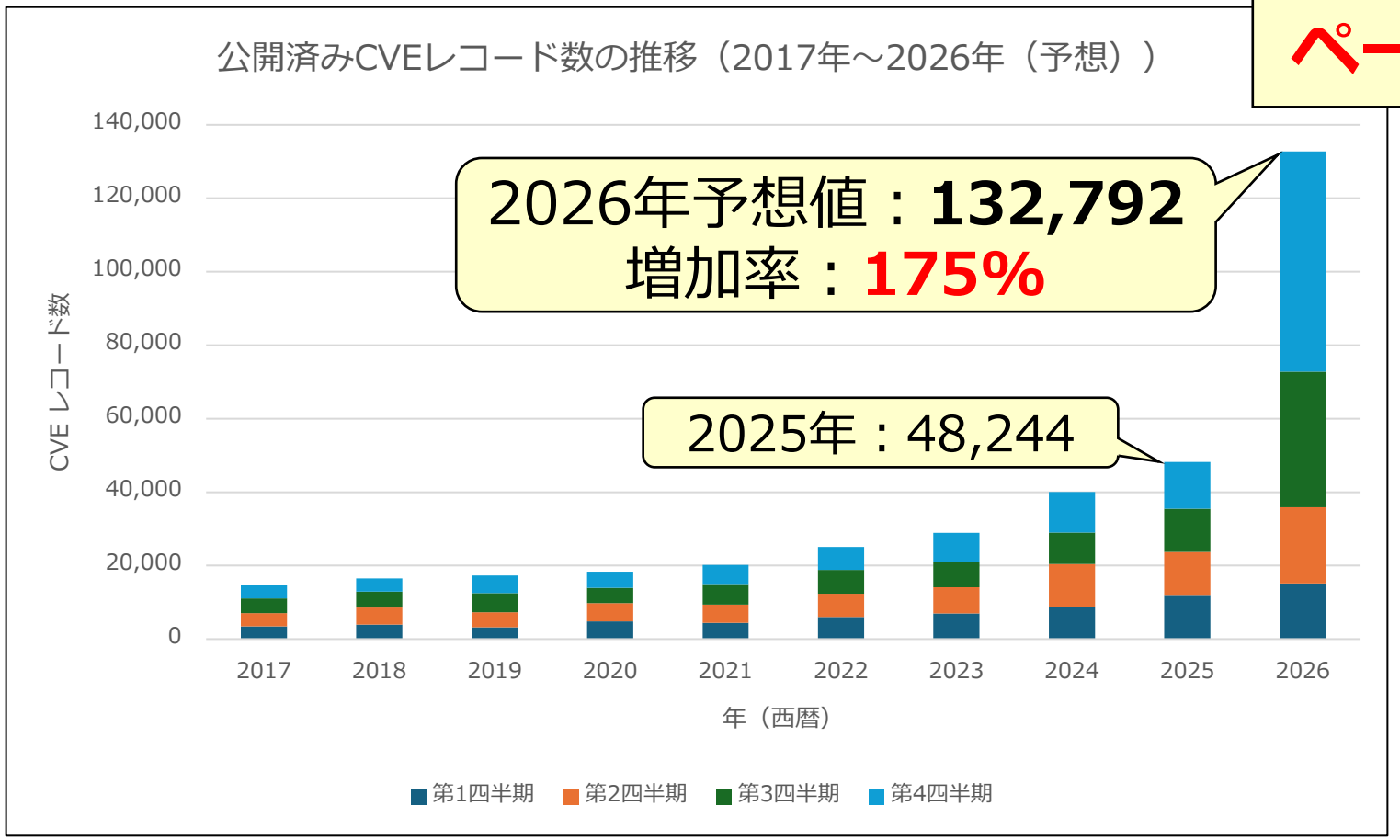


Copyright © 2026 株式会社日本レジストリサービス

公開済みCVEレコード数の推移（予想）

- 今年の11月と12月も**同じペースで増加した場合**

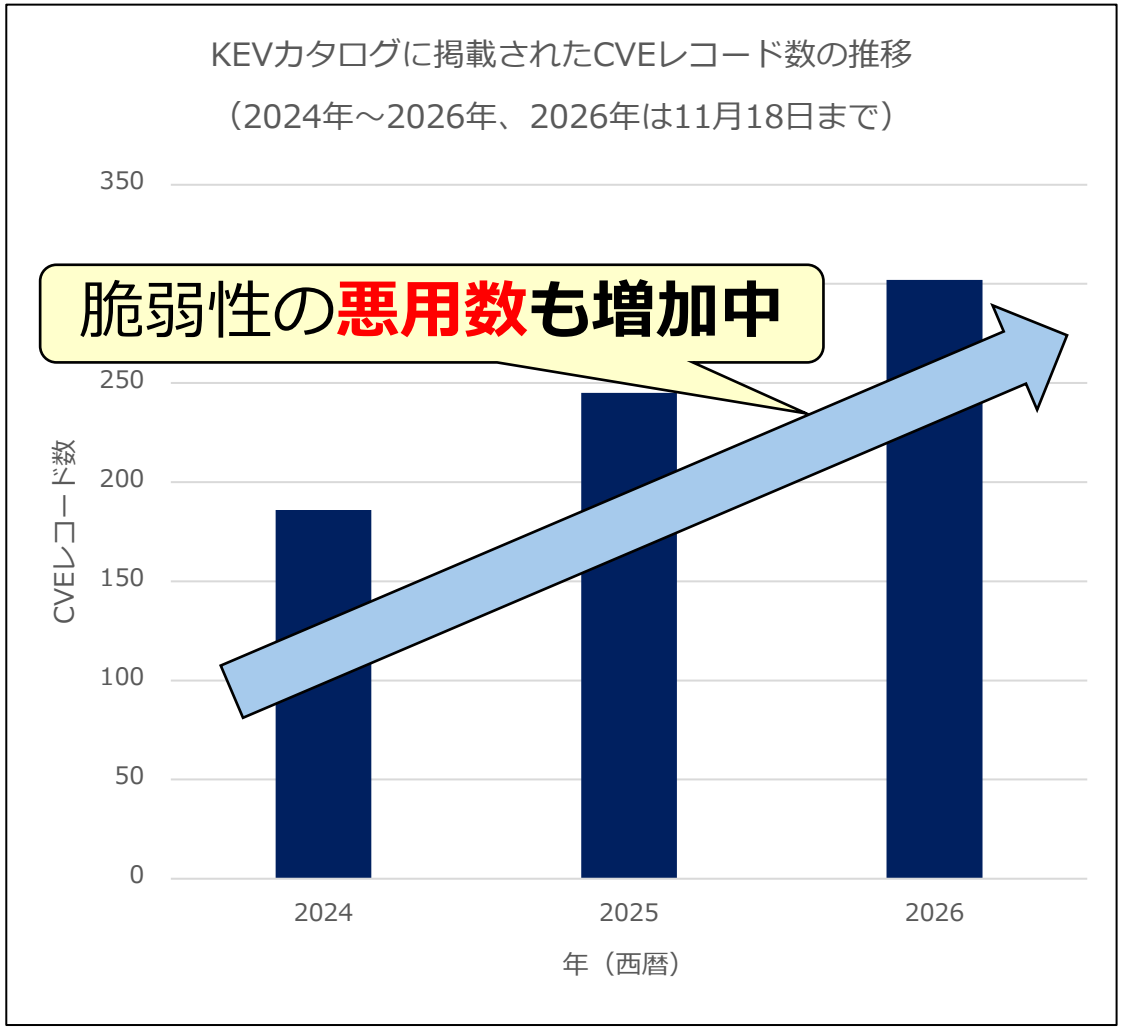
かつてない
ペースで増加中



Copyright © 2026 株式会社日本レジストリサービス

悪用が確認されたCVEレコード数の推移

- 米国サイバーセキュリティ・社会基盤安全保障庁（CISA）のKEVカタログ[*1]に新規掲載されたCVEレコード数の推移



[*1] 悪用が確認された脆弱性をまとめたリスト。

出典：Known Exploited Vulnerabilities Catalog | CISA
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Copyright © 2026 株式会社日本レジストリサービス

本日の内容

1. **DNSにおける現在の脆弱性対応体制**（話者：森下）
2. **DNSの脆弱性において2026年に起こった変化**（話者：熊谷）
3. **この状況にどう立ち向かうべきか**（話者：森下・熊谷）

かつてないペースで脆弱性数が増加している状況を踏まえ、DNSにおける現在の脆弱性対応体制について改めて振り返り、DNSの脆弱性において2026年に起こった変化を分析すると共に、DNSに関わる関係者がこの状況にどう立ち向かうべきかについて考えます。

Copyright © 2026 株式会社日本レジストリサービス

1. DNSにおける現在の脆弱性対応体制

Copyright © 2026 株式会社日本レジストリサービス

このパートの内容

- DNSにおいて**脆弱性対応体制が構築された背景・経緯**を振り返り、**現在の体制の柱**について解説する
  - DNSソフトウェア・製品の増加
  - DNSサービス事業者の増加
  - 情報共有・情報交換・協調体制の確立
  - 有償サポートの整備
  - 現在の脆弱性対応体制の柱
  - まとめ：DNSにおける現在の脆弱性対応体制

Copyright © 2026 株式会社日本レジストリサービス

DNSソフトウェア・製品の増加

- 当初、オープンソースのDNSソフトウェアと言えばBINDであった
- djbdnsを皮切りに**さまざまなソフトウェア・製品**がリリースされ、種類が増加した

オープンソースソフトウェアの例	リリース年
BIND	1985
djbdns	1999
MaraDNS	2001
NSD	2001
PowerDNS Authoritative Server	2002
Unbound	2004
PowerDNS Recursor	2005
Knot DNS	2011
Knot Resolver	2016
bowline	2022

プロプライエタリ・製品の例	リリース年
Microsoft DNS Server	1996
Infoblox DNS Appliance （現：Infoblox Trinzic）	2000
Nominum ANS （現：Akamai DNSi AuthServe）	2002
Nominum CNS （現：Akamai DNSi CacheServe）	2002
XACK DNS	2012

Copyright © 2026 株式会社日本レジストリサービス

DNSサービス事業者の増加

- 並行して、**DNSサービスを提供する事業者**も増加した
  - **パブリックDNSサービス** ＝ **フルリゾルバー**のサービスを提供
  - **マネージドDNSサービス** ＝ **権威DNSサーバー**のサービスを提供

パブリックDNSサービスの例	リリース年
Cisco OpenDNS	2006
Google Public DNS	2009
Quad9	2017
1.1.1.1	2018
IIJ Public DNSサービス	2019

マネージドDNSサービスの例	リリース年
PCH Anycast DNS	1997
DigiCert UltraDNS	1999
DynECT Managed DNS （現：Oracle Cloud Infrastructure DNS）	2008
Amazon Route 53	2010
Cloudflare DNS	2010
IBM NS1 Connect	2013
Google Cloud DNS	2015

Copyright © 2026 株式会社日本レジストリサービス

情報共有・情報交換・協調体制の確立

- DNSソフトウェアベンダー・サービス事業者が増えたことで、**ベンダー・事業者をまたがる形での情報共有・情報交換・協調**が必要になった
- いくつかの**インシデント対応**を契機として、現在につながる情報共有・情報交換・協調の体制が確立されていった
  - ルートサーバーへのDDoS攻撃への対応（2002年）
  - カミンスキー型攻撃手法への対応（2008年）
  - KeyTrapへの対応（2023～2024年）

Copyright © 2026 株式会社日本レジストリサービス

ルートサーバーへのDDoS攻撃への対応

- 2002年に発生し、13系列中7系列のサービスに大きな影響を及ぼした
- 運用コミュニティの連携・情報共有の場として、**DNS-OARC**の設立が進められた

地球規模でDNSをハッカー攻撃から守るための非営利団体「OARC」が発足
<https://internet.watch.impress.co.jp/cda/news/2003/10/21/812.html>

「今回のOARC発足は**1年前のDNSルートサーバーに対するハッカー攻撃を受けて動きを進めてきた**ものだ。」

Proposal - CAIDA
<https://www.caida.org/funding/dns-itr/proposal/>

“Incident Response. **The OARC provides a forum for the DNS operations community to interact during attacks or other incidents that affect global DNS operations.** Stringent confidentiality requirements and secure communications will support sharing of proprietary information on a bilateral basis.”
（参考訳）「インシデント対応。**OARCは、グローバルなDNS運用に影響を及ぼす攻撃やその他のインシデント発生時に、DNS運用コミュニティが連携するための場を提供する。**厳格な機密保持要件と安全な通信手段により、双方向ベースでの専有情報の共有が支援される。」

Copyright © 2026 株式会社日本レジストリサービス

カミンスキー型攻撃手法への対応

- 2008年に発表された、キャッシュポイズニングの効率を高める脆弱性
- 本インシデントを契機として、現在につながる**関係者間の対応体制**が整備された
  - DNSソフトウェアベンダーをまたがる形での**情報共有・情報交換**
  - 脆弱性情報・パッチの公開における**ベンダー間の協調**
    - 複数のベンダーが脆弱性情報とパッチを同時公開
  - **JP*（JPCERT/CC、JPNIC、JPRS）**における情報共有・協調
    - DNS関連の脆弱性情報公開時の連携、文書間での相互リンクの実施など

Copyright © 2026 株式会社日本レジストリサービス

KeyTrapへの対応

- 2024年に発表された、DNSSEC検証によるDoS攻撃を図る脆弱性
  - プロトコル仕様の弱点を突いた攻撃、**複数のDNSソフトウェア**が対象
- 構築された体制を活かした**情報共有・交換・協調**が実施された

The Harder You Try, The Harder You Fail:
The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC
<https://dl.acm.org/doi/10.1145/3658644.3670389>

“We initiated the disclosure process on November 2. 2023, following which **a group was formed of 31 participants**, consisting of vendors of DNS software, operators of DNS/Cloud/CDN, and IETF experts. The group communicates over **a closed DNS OARC channel** established for disclosure and mitigations of our attacks.”
（参考訳）「我々は2023年11月2日に開示プロセスを開始した。その後、DNSソフトウェアベンダー、DNS／クラウド／CDNの運用者、及びIETFの専門家からなる、**計31名の参加者によるグループが結成**された。このグループは、我々の攻撃に関する開示および緩和策のために設置された**非公開のDNS OARCチャネル**を通じて連絡を取り合っている。」

Copyright © 2026 株式会社日本レジストリサービス

有償サポートの整備

- オープンソースDNSソフトウェアにおいて、**有償サポート**が整備された
- 2000年代のBIND Forum、PowerDNSの商用サポートが先駆け
- 2010年代に**主要4ベンダー**が有償サポートプログラムを開始
  - ISC：Professional Support
  - NLnet Labs：Professional Services
  - PowerDNS.COM：Commercial Support
  - CZ.NIC：Professional Support

Copyright © 2026 株式会社日本レジストリサービス

現在の脆弱性対応体制の柱

- 脆弱性情報の**事前通知**と関係者間の**情報共有・交換・協調**が、対応体制の柱になっている
  - 脆弱性情報の**事前通知**
    - 有償サポートプログラムの顧客：5～10営業日前に事前通知
      - JPRSはこの情報を使って脆弱性情報を事前作成し、当日に公開
    - BIND：5営業日前にbind-announceメーリングリストで事前通知
      - セキュリティ修正があること、その公開日、複数かどうか（内容は通知されない）
  - 重大な脆弱性における関係者間の**情報共有・交換・協調**
    - 対象を限定した情報共有・交換
    - 公開日時の調整、脆弱性情報とパッチの同時公開

Copyright © 2026 株式会社日本レジストリサービス

まとめ： DNSにおける現在の脆弱性対応体制

- 背景：**DNSソフトウェア・製品・サービスの多様化**
- インシデント対応を契機として、**情報共有・交換・協調体制が確立**
- 2010年代にオープンソースDNSソフトウェアの**有償サポート**が整備
- 体制の柱：情報の**事前通知**と関係者間の**情報共有・交換・協調**

25年以上にわたる対応により、現在の体制が整備された

Copyright © 2026 株式会社日本レジストリサービス

2. DNSの脆弱性において
2026年に起こった変化

Copyright © 2026 株式会社日本レジストリサービス

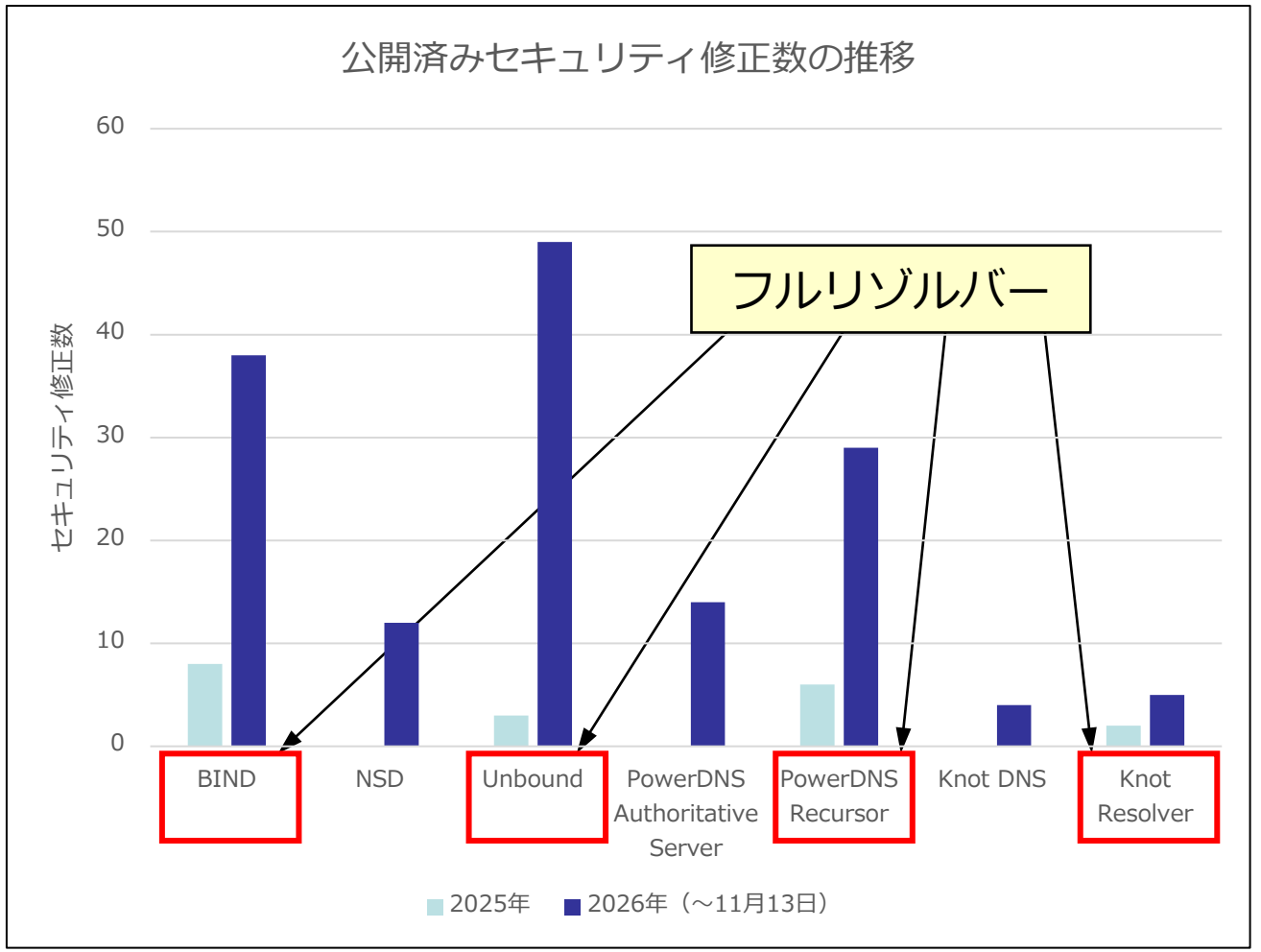
このパートの内容

- DNSの脆弱性において、**2026年に起こった変化**を解説する
  - 脆弱性数の大幅な増加
  - BIND以外の脆弱性数の増加
  - 脆弱性のパターンの増加
  - 影響が大きい脆弱性の頻度の増加
  - 特定の報告者による脆弱性報告の増加
  - まとめ：2026年に起こった変化

Copyright © 2026 株式会社日本レジストリサービス

脆弱性数の大幅な増加

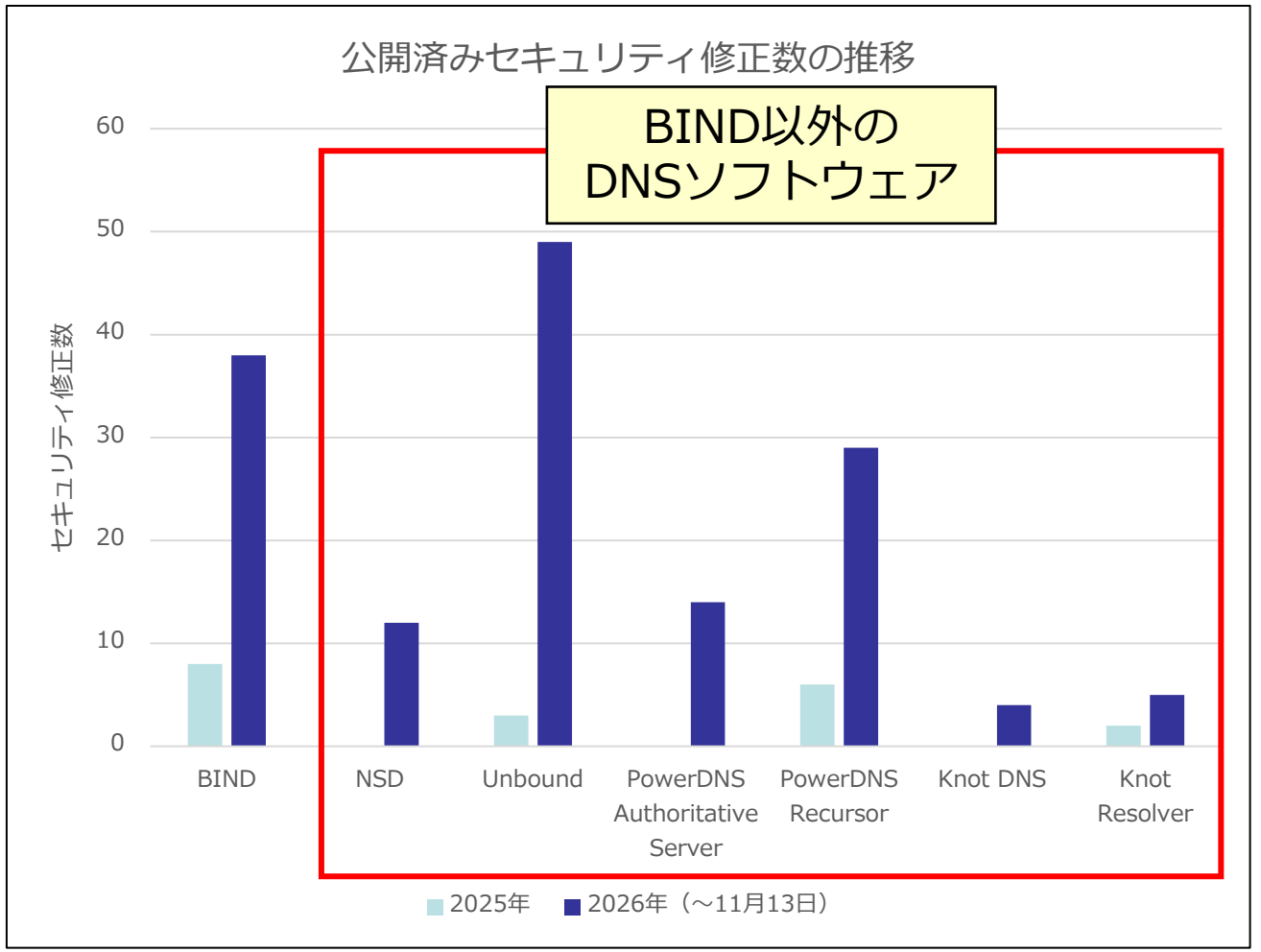
- 2025年に比べ、脆弱性数が**大幅に増加**
- 脆弱性が発生する**箇所・処理の傾向は以前と同様**
  - **フルリゾルバー**の**ステップ数が多い処理**や、**以降の動作に影響を及ぼす処理**の脆弱性が目立っている



Copyright © 2026 株式会社日本レジストリサービス

BIND以外の脆弱性数の増加

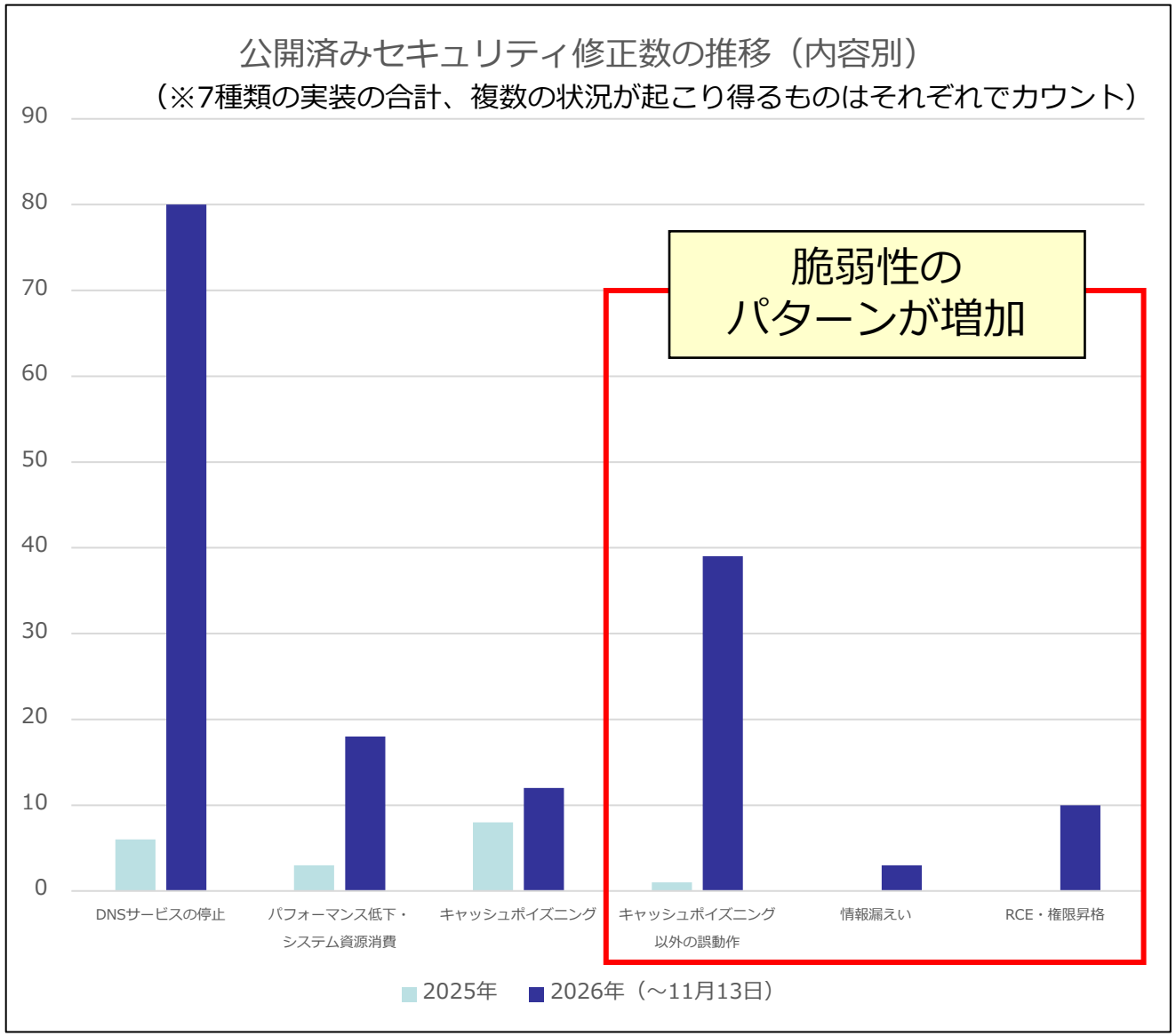
- **BIND以外のDNSソフトウェア**の脆弱性数も大幅に増加
  - 2026年は11月13日時点において、Unboundの脆弱性数がBINDの脆弱性数を上回っている
  - Knot DNS、Knot Resolverの脆弱性数は今のところ少ない
    - バグ修正数はそれなりにあるが、脆弱性に至っていない



Copyright © 2026 株式会社日本レジストリサービス

脆弱性のパターンの増加

- 2025年はDNSサービスの停止に加え、清華大学の研究グループが発表したキャッシュポイズニング脆弱性が目立った
- 2026年はDNSサービスの停止の大幅な増加に加え、キャッシュポイズニング以外の誤動作・情報漏えい・RCEなど、**脆弱性のパターンが増加**している



Copyright © 2026 株式会社日本レジストリサービス

影響が大きい脆弱性の頻度の増加

- 内容の多様化に伴い、従来はほとんど見られなかった**CVSSスコアが8.0を超える、影響が大きい脆弱性**の頻度が増加
- 2026年に公開された、CVSSスコアが8.0を超える脆弱性の例
  - BIND：CVE-2026-13321（CVSS v3.1：8.6）
    - DNSSEC不在証明の実装ミスを利用し、存在するドメイン名を存在しないと誤認させる
    - **広範囲のドメイン名に対するDoS攻撃**が可能　誤動作を利用したDoS攻撃
  - Unbound：CVE-2026-81642（CVSS v4.0：9.1）
    - DNSSEC検証の実装ミスを利用し、ヒープベースのバッファオーバーフローを誘発させる
    - 最悪の場合、**リモートコード実行（RCE）**可能　サーバーの侵害

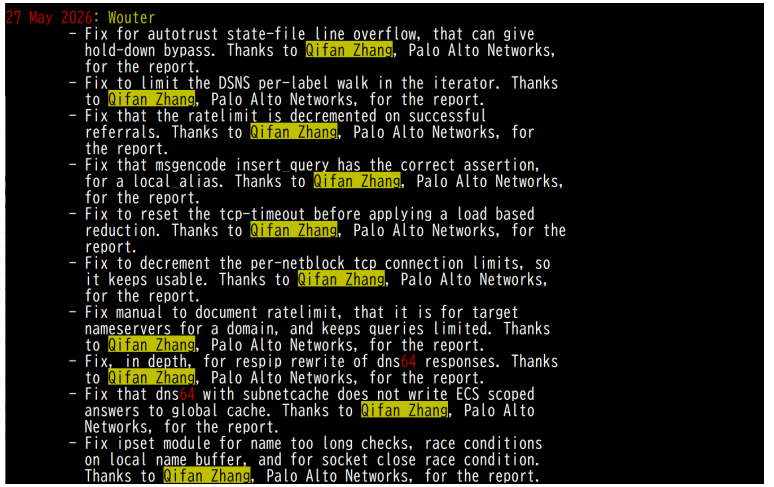
Copyright © 2026 株式会社日本レジストリサービス

特定の報告者による脆弱性報告の増加

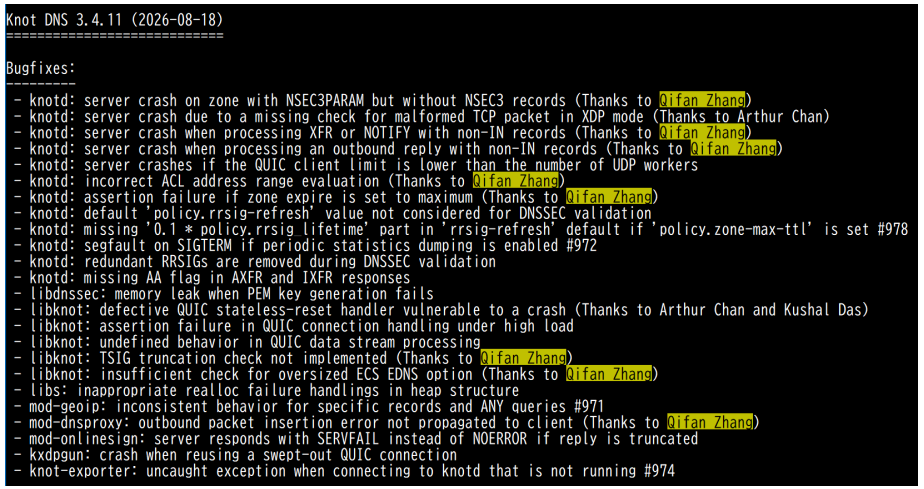
- **特定の報告者が多数の脆弱性を報告する**傾向が顕著に
  - 2026年5月頃から、セキュリティ研究者Qifan Zhang氏の活動が際立っている
    - BIND：38件中5件
    - NSD：12件中10件
    - Unbound：49件中35件、など

※2026年（～11月13日）に公開された脆弱性のうち、同氏が謝辞にクレジットされている件数。

  - 同氏は脆弱性と判定されなかったものも含め、複数のDNSソフトウェアの多数のバグを報告
    - 付属のドキュメントに同氏への多数の謝辞あり



UnboundのChangelog（抜粋）



Knot DNSのNEWS（抜粋）

Copyright © 2026 株式会社日本レジストリサービス

Qifan Zhang氏

- 研究分野
  - **DNS、セキュリティのための機械学習**
- 研究成果（抜粋）
  - 2024年に問い合わせ・応答・ファジングで**リゾルバーの脆弱性を自動発見するツール**「ResolverFuzz」を発表
  - 2026年にDNSSECのワイルドカードの取り扱いの**仕様の不備**を指摘、改善提案を**IETFのインターネットドラフトとACM CCS 2026の論文で発表**

Signer-Zone Containment for DNSSEC Wildcard Validation
<https://datatracker.ietf.org/doc/draft-zhang-dnssec-wildcard-validation/>

Mind the Gap: Cross-RFC Formal Analysis Exposes DNSSEC's Hidden Vulnerabilities | Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security
<https://dl.acm.org/doi/10.1145/3830454.3846592>



2020年に上海科技大学を卒業、2025年にカリフォルニア大学アーバイン校でPh.D.取得

引用元：<https://qifanz.com/>

Copyright © 2026 株式会社日本レジストリサービス

まとめ：2026年に起こった変化

- LLM/AIの進化によって欠陥を見つけやすくなり、かつその欠陥を突くPoCを実装しやすくなったことで**難易度が下がり、**以下の状況が発生
  - 脆弱性数が**大幅に増加**、「BINDから卒業すればOK」という時代は**完全に終了**
  - 脆弱性の**パターンが増加**
  - 影響が大きい脆弱性の**頻度が増加**

1年足らずで、脆弱性の状況が激変した

- 欠陥を発現させる**方法を発見できる者**は、**今のところまだ多くない**
  - 「**優れた者が優れた道具を手に入れるとどうなるか**」が実証されている状態

Copyright © 2026 株式会社日本レジストリサービス

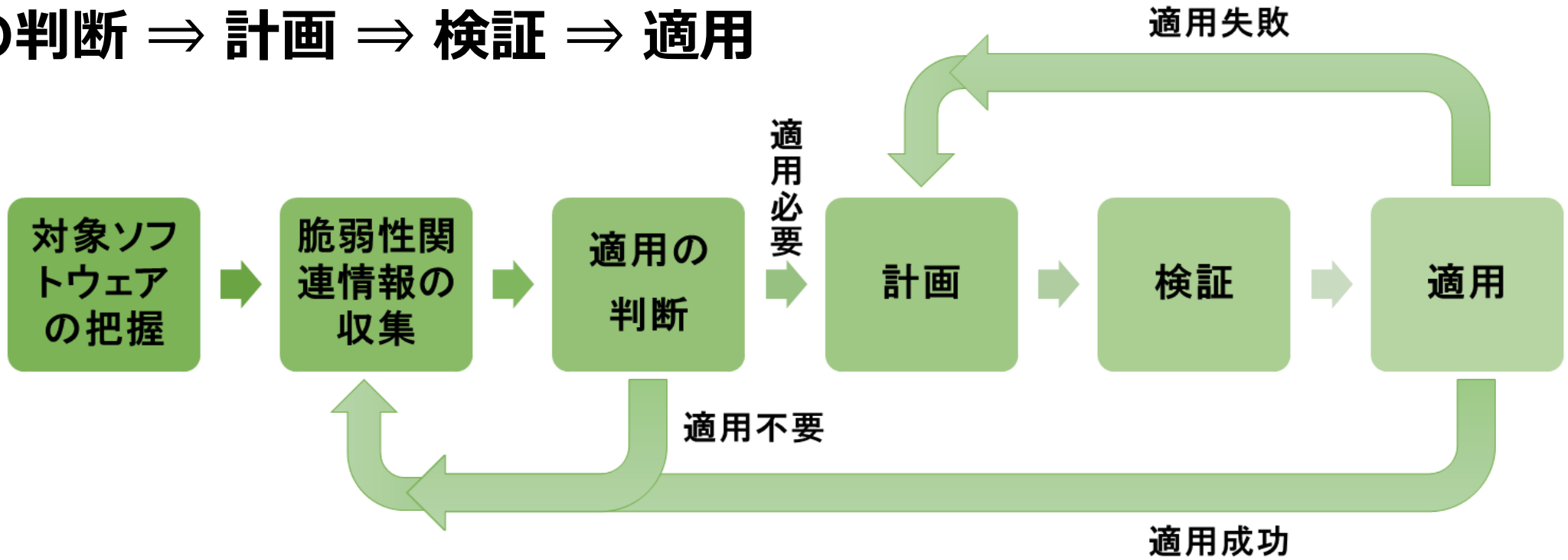
3. この状況にどう立ち向かうべきか

ここからはご好評いただいている、
森下と熊谷の掛け合いで進めます。

Copyright © 2026 株式会社日本レジストリサービス

おさらい：現在の脆弱性対応の流れ

- 脆弱性ごとに、以下の対応が実行される
  - **適用の判断 ⇒ 計画 ⇒ 検証 ⇒ 適用**

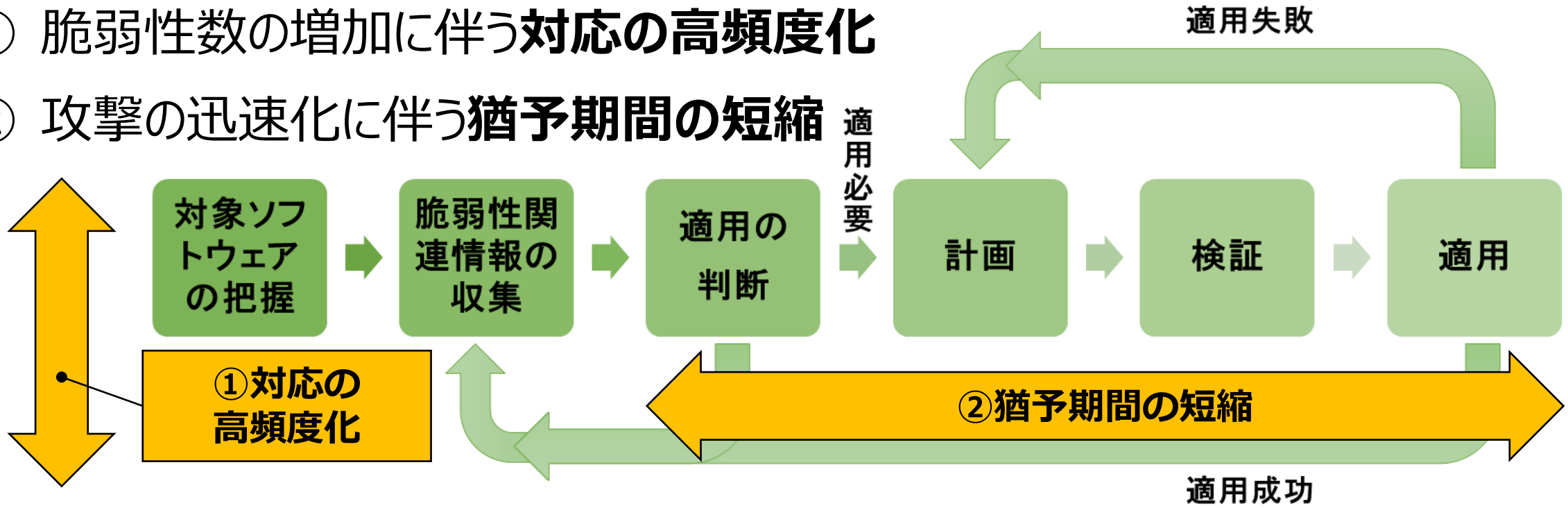


引用元：IPAテクニカルウォッチ「脆弱性対策の効果的な進め方（ツール活用編）」
<https://www.ipa.go.jp/security/reports/technicalwatch/20190221.html>

Copyright © 2026 株式会社日本レジストリサービス

今起こっていること

- 以下の2項目が**急速に**進んでいる
  - ① 脆弱性数の増加に伴う**対応の高頻度化**
  - ② 攻撃の迅速化に伴う**猶予期間の短縮**



もともとあったトレンドが、LLM/AIで急加速した

Copyright © 2026 株式会社日本レジストリサービス

DNSソフトウェアベンダーの対応状況

- 新機能開発の優先度を下げ、**脆弱性対応に注力**している
  - BIND 9.22のリリースを延期し、サポートバージョンを9.20に一本化（ISC）
  - 「ほぼ全チームがバグ修正のリリースで手一杯で、出口が見えない」（NLnet Labs）

“If you’re wondering why you haven’t seen any major new features in our software since the beginning of this year, it’s because by now **almost all of our teams are maxed out with releasing bug fixes**, in some cases in close coordination with other software vendors. There have been times that the stream seemed to dry up and **we thought we reached the end of the tunnel, but then a new AI model was released and the process started over**.”
（参考訳）
「今年に入ってからわれわれのソフトウェアに目立った新機能が追加されていない理由について疑問に思っているかも知れないが、それは今、**ほぼすべてのチームがバグ修正のリリースで手一杯になっている**ためである。場合によっては、他のソフトウェアベンダーと緊密に連携しながら対応していることもある。流れが途絶えたように見え、**トンネルの出口に達したかと思われたことも何度かあったが、新しいAIモデルがリリースされるたびに、そのプロセスが最初から繰り返されてきた**。」

引用元：Maintaining the love for coding in the time of AI
<https://blog.nlnetlabs.nl/maintaining-the-love-for-coding-in-the-time-of-ai/>

脆弱性対応に注力しているが、まだ出口が見えない状況

Copyright © 2026 株式会社日本レジストリサービス

脆弱性対応におけるDNSサービスの特徴

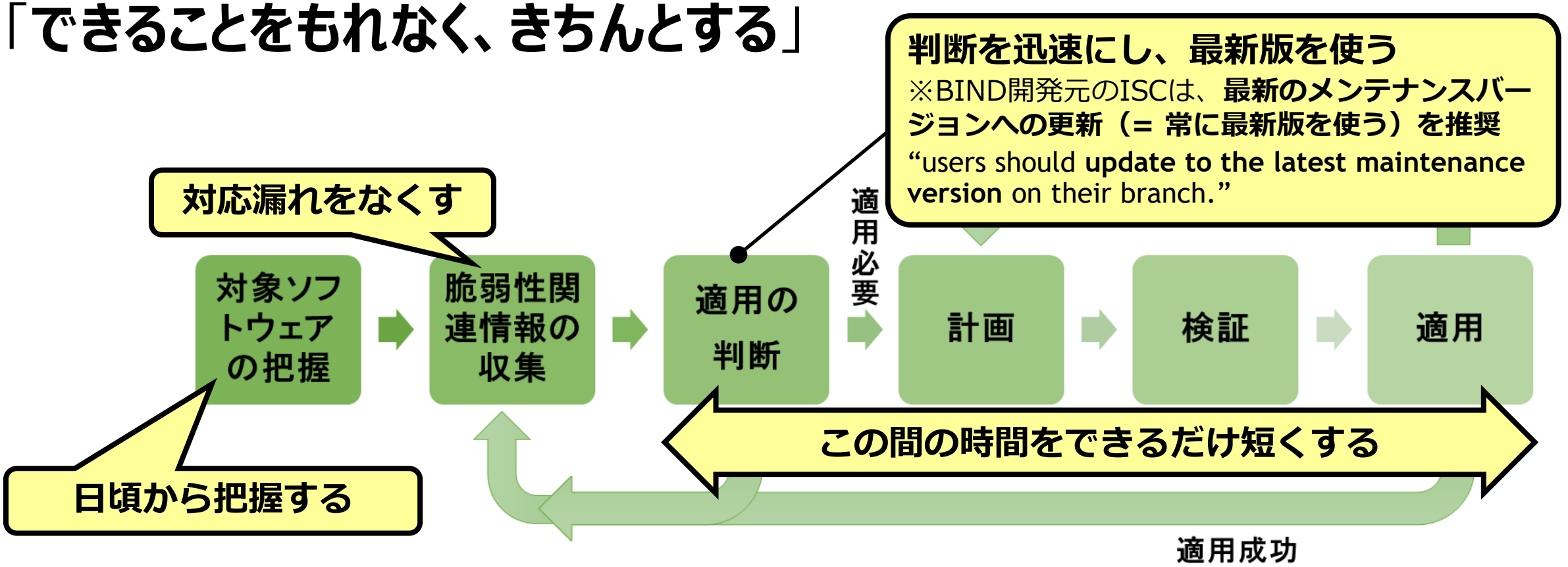
- 「**攻撃に備えてサービスを止める**」という対応が困難
  - DNSは**動かし続ける必要がある**重要なサービスの一つ
- しかし、きちんと運用することで**ロバストネス（堅牢性）**が高められる
  - ロバストネスがプロトコルレベルで考慮されている
  - 複数のソフトウェア実装・サービス・TLDが存在し、冗長化・多様化できる
  - IP Anycastなど、ロバストネスを高める技術が開発・利用されている

DNSは止めることができない重要なサービスであるが、
きちんと運用することでロバストネスが高められる

Copyright © 2026 株式会社日本レジストリサービス

DNS運用者がまずすべきこと

- 「できることをもれなく、きちんとする」



Copyright © 2026 株式会社日本レジストリサービス

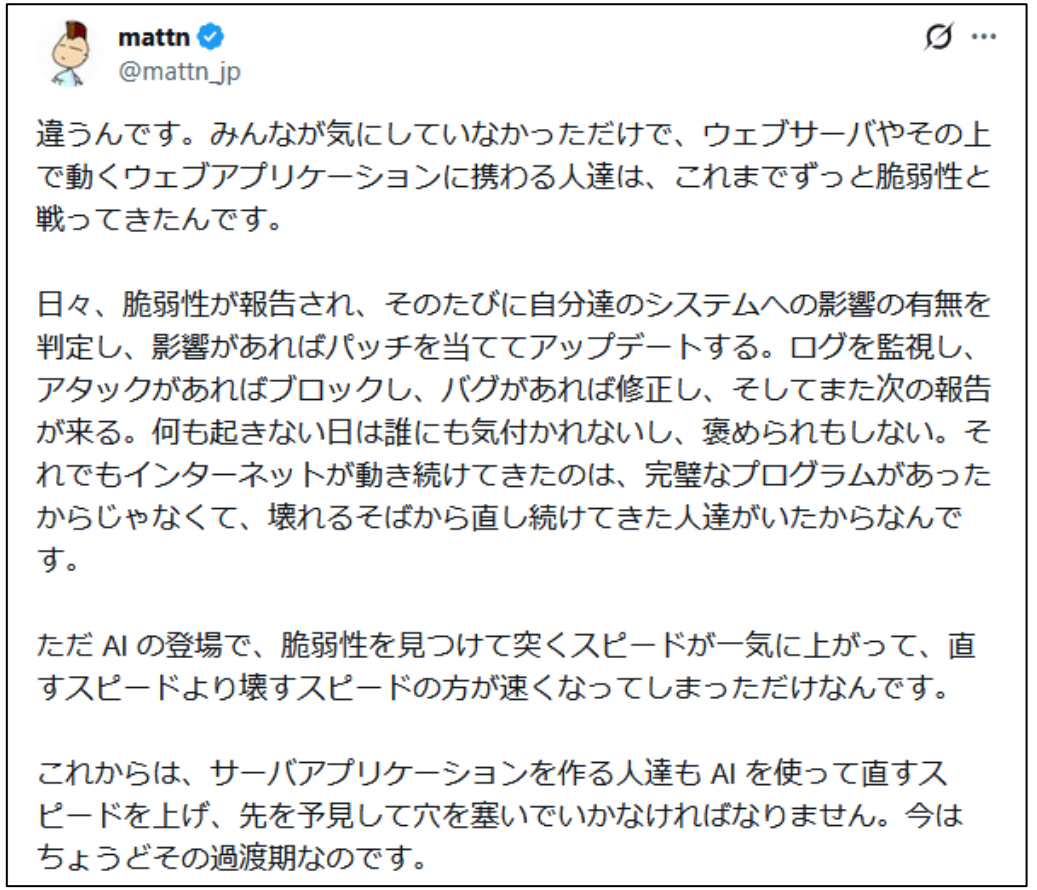
次に進むヒントになるかもしれないこと

- 松本泰弘（mattn）氏のX投稿
  - 「ただAIの登場で、脆弱性を見つけて突くスピードが一気に上がって、直すスピードより壊すスピードの方が速くなってしまっただけなんです。」

直すスピードより壊すスピードの方が速くなった

  - 「これからは、サーバアプリケーションを作る人達もAIを使って直すスピードを上げ、先を予見して穴を塞いでいかなければなりません。今はちょうどその過渡期なのです。」

直すスピードの向上と先を見越した対応が必要になる



mattn
@mattn_jp

違うんです。みんなが気にしていなかっただけで、ウェブサーバやその上で動くウェブアプリケーションに携わる人達は、これまでずっと脆弱性と戦ってきたんです。

日々、脆弱性が報告され、そのたびに自分達のシステムへの影響の有無を判定し、影響があればパッチを当ててアップデートする。ログを監視し、アタックがあればブロックし、バグがあれば修正し、そしてまた次の報告が来る。何も起きない日は誰にも気付かれないし、褒められもしない。それでもインターネットが動き続けてきたのは、完璧なプログラムがあったからじゃなくて、壊れるそばから直し続けてきた人達がいたからなんです。

ただ AI の登場で、脆弱性を見つけて突くスピードが一気に上がって、直すスピードより壊すスピードの方が速くなってしまっただけなんです。

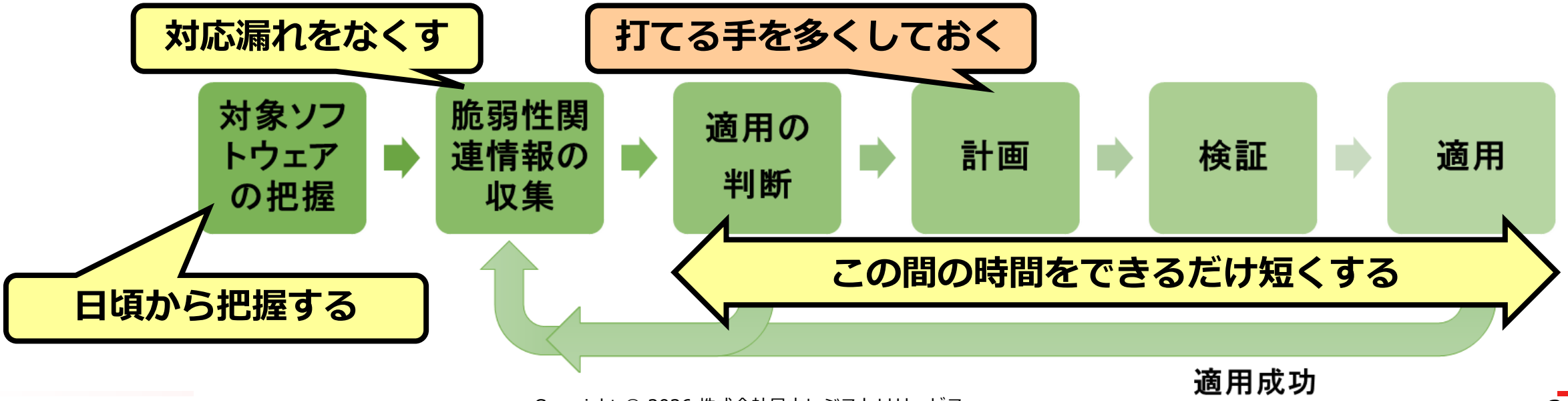
これからは、サーバアプリケーションを作る人達も AI を使って直すスピードを上げ、先を予見して穴を塞いでいかなければなりません。今はちょうどその過渡期なのです。

引用元：<https://x.com/mattn_jp/status/2113197278853022166>

Copyright © 2026 株式会社日本レジストリサービス

DNS運用者がめざす方向

- 「**直すスピードの向上と先を見越した対応が必要になる**」のは、DNS運用者も同じ
  - 黄色い部分のスピードを、**壊すスピードよりも速くする**
  - 複数の対応を**事前に計画・準備**し、**打てる手を多くしておく**



Copyright © 2026 株式会社日本レジストリサービス

「直すスピードを速くする方法」の候補

- 意思決定の迅速化
- トリアージの迅速化・簡略化
- パッチ適用の自動化
- 訓練・シミュレーションによるパッチ適用の練度の向上
- 脆弱性対応の計画・検証・適用へのLLM/AIの活用、など

いずれも重要な項目であるが、すべてを即座に実現することには困難を伴う

Copyright © 2026 株式会社日本レジストリサービス

「打てる手」の候補

- 実装・サービスにおける多様性の確保
  - 複数の実装・サービスを組み合わせた運用
- ワークアラウンドの確保
  - パッチの適用までに実施可能な緊急対策の事前策定・準備
- 提供する機能の切り分け・制限
  - 優先度の低い機能の提供終了、提供範囲の制限
- 脆弱性の発生が少ないソフトウェアの選択
  - Knot DNS/Knot Resolverは現在の有力候補だが、状況は変わり得る

こうした「地に足を着けた確実な運用」が、確実なリスクの低減につながる

Copyright © 2026 株式会社日本レジストリサービス

まとめ：この状況にどう立ち向かうべきか

- DNSはロバストネスを高められるサービスであり、**地に足を着けた確実な運用を継続すること**が、既存の脅威に対する**確実なリスクの低減**につながります。
- そのためには**打てる手を多くし、できる手を確実に打っておく**ことが、有効な対策となります。
- その上で、将来はDNSの運用においても「**直すスピードを壊すスピードよりも速くする方法**」を、早急に確立する必要があります。

Copyright © 2026 株式会社日本レジストリサービス

おわりに

- 今回は「**かつてない脆弱性数の増加にどう立ち向かうべきか**」と題し、**脆弱性に起こっている変化**を分析すると共に、DNSに関わる関係者が**この状況にどう立ち向かうべきか**について考えました。
- 古生物学の「**P-T境界**」や「**K-Pg境界**」に匹敵する**環境の激変**に対応するため、25年以上かけて整備された現在の体制を刷新する、**まったく新しい脆弱性対応体制**が必要になるかも知れません。
- P-T境界やK-Pg境界では、**激変を生き延びた生物が繁栄**しました。

みんなで力を合わせて、激変を乗り切りましょう！

Copyright © 2026 株式会社日本レジストリサービス

最後までお聞きいただき
ありがとうございました！

<https://jprs.jp/tech/>

アンケートにご回答お願いします！

@JPRS_official　JPRSofficial　JPRSpress

Copyright © 2026 株式会社日本レジストリサービス