【JNSA】活動報告会パネルディスカッション
「大量パッチ時代の脆弱性対応」
～フロンティアAI時代に我々はどう対応すべきか？～

2026/7/24

川口 修司

独立行政法人
情報処理推進機構　セキュリティセンター

自己紹介

1990-2017 株式会社三菱総合研究所

情報セキュリティをはじめとする情報通信分野の市場・技術・制度に関する
政策提言、調査研究、コンサルティングに従事

2003-2005 経済産業省 情報セキュリティ政策室(出向)

2005-2008 独立行政法人メディア教育開発センター 特任教授(兼務)

2013-現在 東京理科大学 非常勤講師(兼務)

2017-現在 独立行政法人情報処理推進機構

セキュリティセンター　情報分析官

対処調整部 対処支援グループ

サイバー情勢研究部 運用グループ

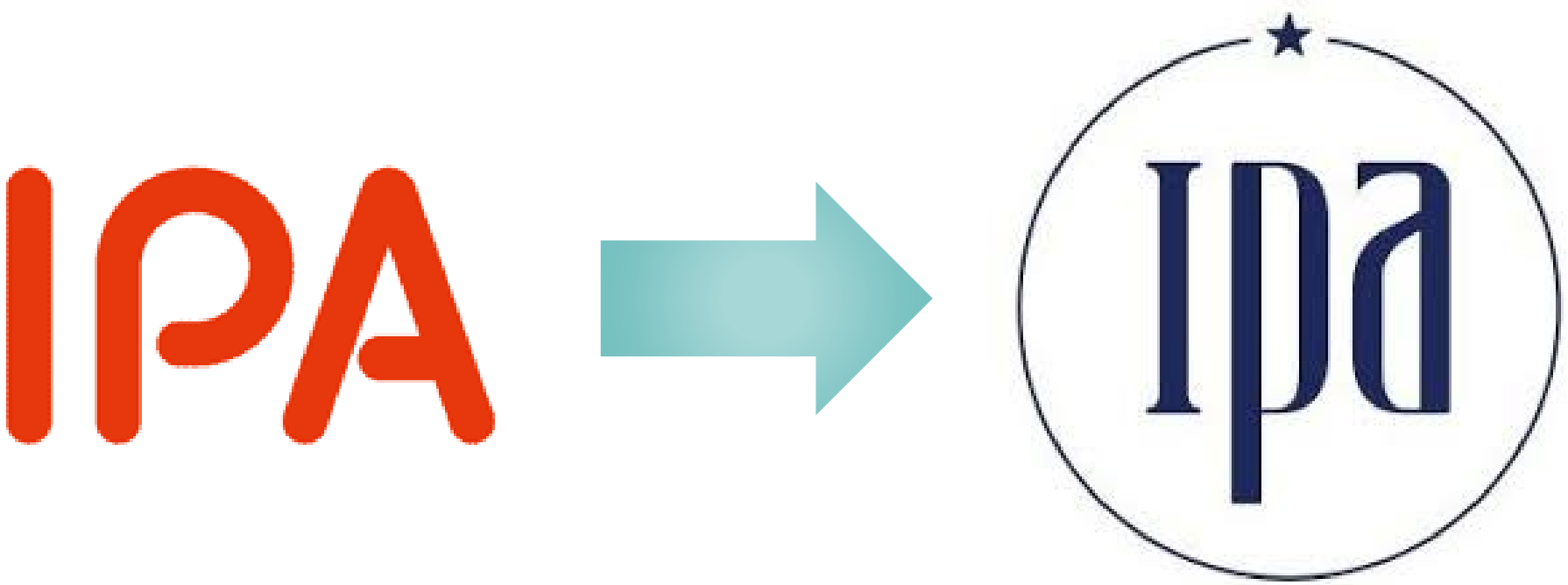
早期警戒担当

デジタル基盤センター

デジタルエンジニアリング部 AIシステムグループ

出所：IPA「パスワード－もっと強くキミを守りたい－」
https://warp.ndl.go.jp/web/20260111120758/https://www.ipa.go.jp/security/munekyun-pw/

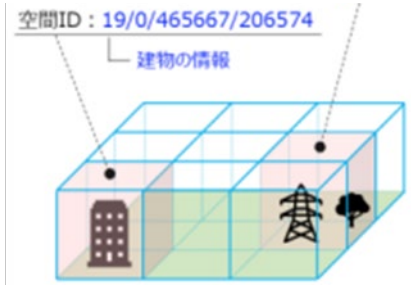
Rebranding



独立行政法人情報処理推進機構（IPA）のご紹介

- 日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人です。
- 「人材」、「セキュリティ」、「デジタル基盤」の3つの中核事業を通じて、誰もが安心してITのメリットを実感できる「頼れるIT社会」の実現を目指しています。

Ouranos Ecosystem



DX・イノベーションで
新たな価値を生む
デジタル人材の育成を加速

社会全体のアーキテクチャ設計
およびデータスペース整備による
Society 5.0実現のための基盤を提供

DX認定
Digital Transformation Certification

リアルとサイバーの融合でリスクが高まる
サイバーセキュリティの強化を実現

MITOU

JC-STAR

セキュリティ分野の取組方針

- 2022年の「国家安全保障戦略」の閣議決定を踏まえ、第五期中期計画（2023年～）で、初めて**国家の安全保障・経済安全保障の確保への貢献**が規定されました。

【第五期中期計画（粋） 2023年4月～】

・・・第五期中期目標期間において機構は、官民連携の最前線として、関係省庁等との連携を強化しつつ、サイバー脅威情報の集約のみならず分析・評価能力の強化を通じて「サイバー状況把握力」の強化を図り、これによって、精度の高い脅威評価と多面的なサイバーセキュリティに関する課題解決提案を行い、もって国家の安全保障・経済安全保障の確保に貢献する。・・・

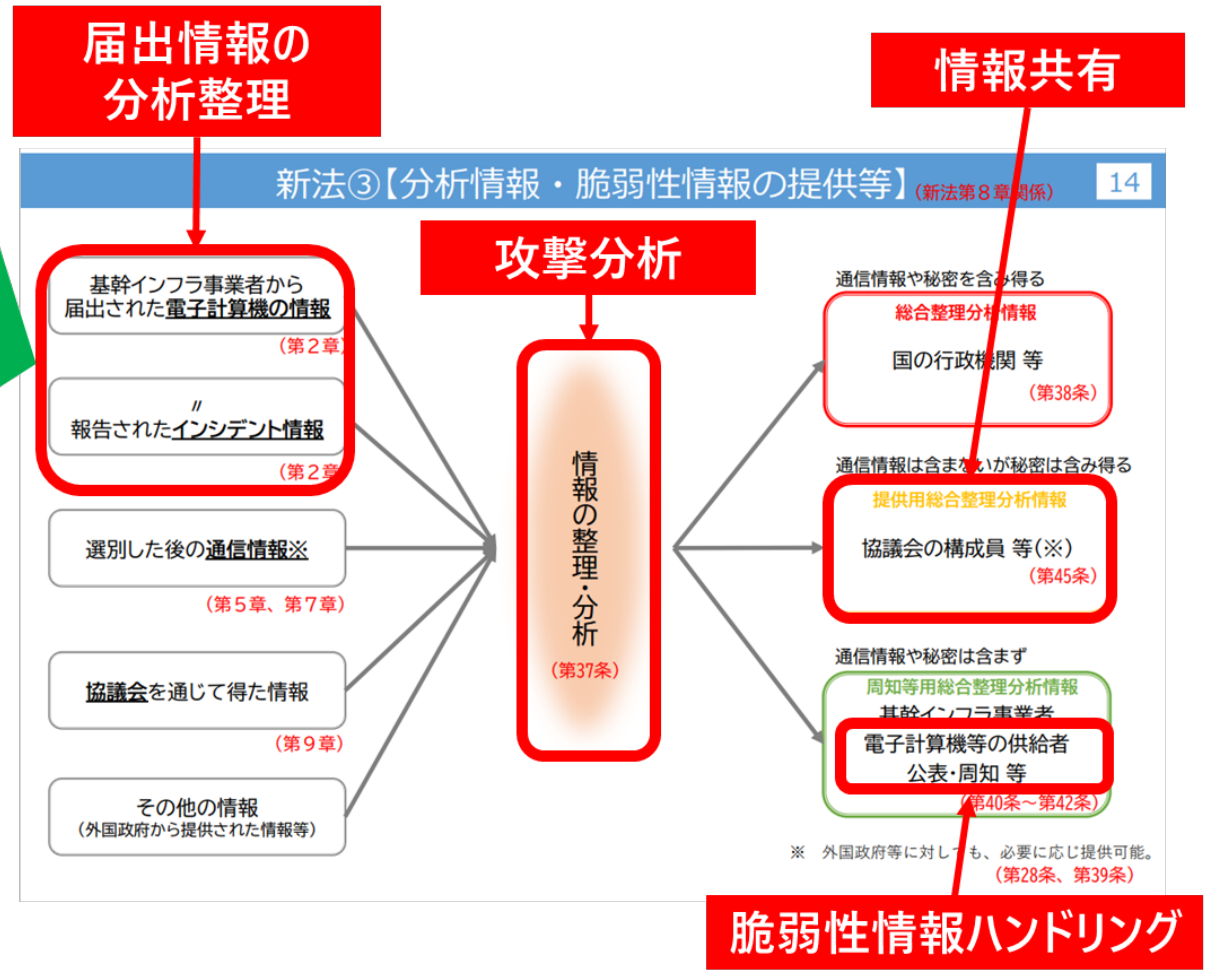
官民連携の最前線として

政府では、共有が難しい脅威情報の背景や解釈を提供
IPAが現場で得た脅威情報を、直接かつ一足早く提供

「サイバー対処能力強化法」におけるIPAの位置付け

- 2025年5月に成立した**「サイバー対処能力強化法」**において、IPAは、**政府が集約した情報の整理・分析及び周知普及等を法定事務として行う**ことになっています。

https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf



セキュリティセンターにおけるサイバー状況把握の体制

- 国の安全保障、経済安全保障に貢献するため、セキュリティセンターには、**セキュリティ運用を行う部門と、地政学や経済安全保障見地からの情勢分析を行う部門を**設置。
- セキュリティのみならず、地政学・経済安保など多様なバックグラウンドを有する民間、政府（自衛隊や県警など）からの人材で構成。

サイバー情勢分析部門

セキュリティ専門見地と地政学・経済安保見地での統合的な分析

JVN iPedia

脆弱性対策

早期警戒パートナシップ

脆弱性データベース

J-CSIP Initiative for Cyber Security Information sharing Partnership of Japan

APT攻撃関係の情報共有枠組み

制御システムのリスクアセスメント支援

サイバーレスキュー隊[J-CRAT]

APT攻撃の初動対応支援・脅威ハンティング

サイバー分野の経済安全保障

GSOC

不正通信監視（独法等）

サイバーセキュリティお助け隊（中小事業者）

企業向け相談窓口

ウイルス/不正アクセス届出窓口

その他各種オシント情報

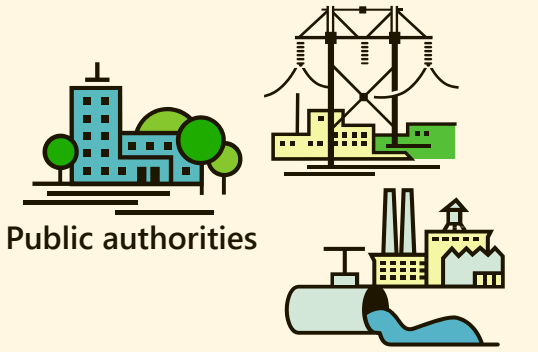
関係機関/組織との連携体制

産業界

サプライチェーン
サイバーセキュリティ
コンソーシアム
SC3

連携協定(2025)

J-CSIP
Initiative for Cyber Security Information sharing Partnership of Japan



経済産業省
Ministry of Economy, Trade and Industry

国家サイバー統括室
National Cybersecurity Office

「サイバー対処能力強化法」に基づく情報の整理分析、対処支援、監視に関する指示

エスカレーション
分析提供

サイバー対処・交流に係る連携

スレットハント活動
初動対応支援

1.5レイヤーでの連携協力

海外機関

政府関係機関

防衛省・自衛隊
MINISTRY OF DEFENSE
連携協定(2024)

警察庁
National Police Agency
連携協定(2023)

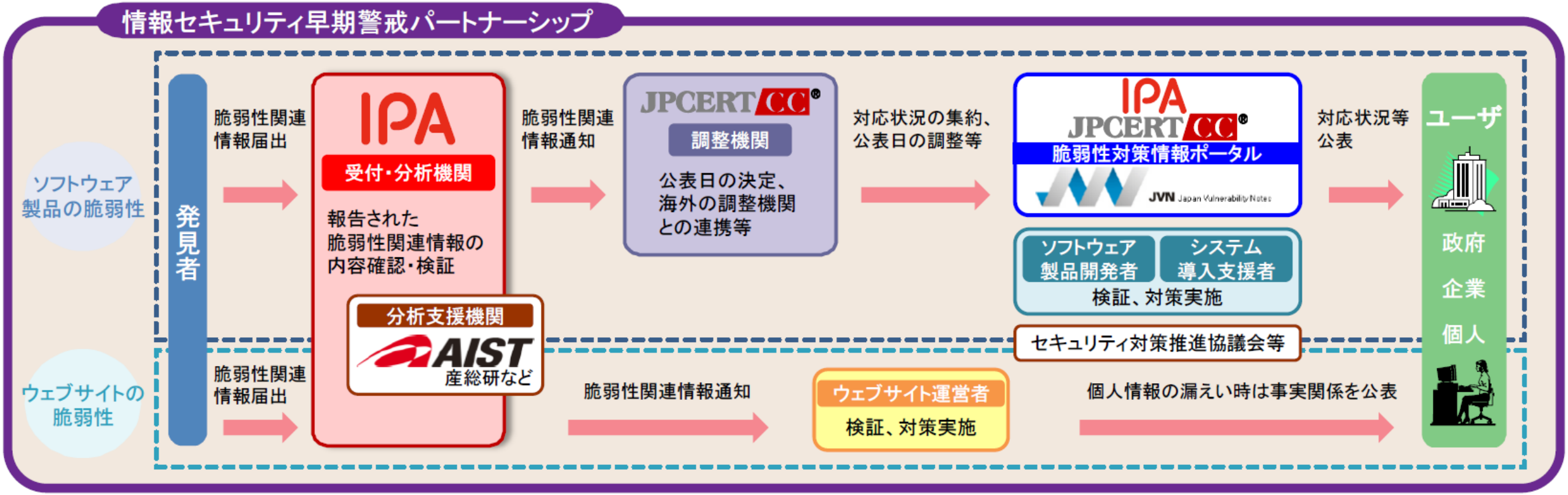
PPC 個人情報保護委員会
Personal Information Protection Commission
連携協定(2023)

JCG 海上保安庁
JAPAN COAST GUARD

・・・

情報セキュリティ早期警戒パートナーシップ（脆弱性関連情報届出制度）

- 2004年7月から「情報セキュリティ早期警戒パートナーシップ」の名称で運用開始。
- 発見者が脆弱性を受付機関（IPA）に届け出れば、製品開発者またはWebサイト運営者が適切に対処してくれる制度。脆弱性情報は、最終的にポータルサイト「JVN」で、対策と一緒に公表される。
- 法制度ではなく、官民連携の自主的な取組として整備。



※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人　JPCERTコーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

出所：IPA「情報セキュリティ早期警戒パートナーシップガイドライン概要日本語版」
https://www.ipa.go.jp/security/guide/vuln/ug65p90000019by0-att/partnership_guideline_overview_jp.pdf

脆弱性関連情報の届出状況

- IPAへの脆弱性関連情報の届出件数(2026年第2四半期)：
  ソフトウェア製品に関するもの 182件、ウェブサイトに関するもの 65件
- 特にソフトウェア製品については、2025年第3四半期以降**4期連続で100件超の届出**となっている。

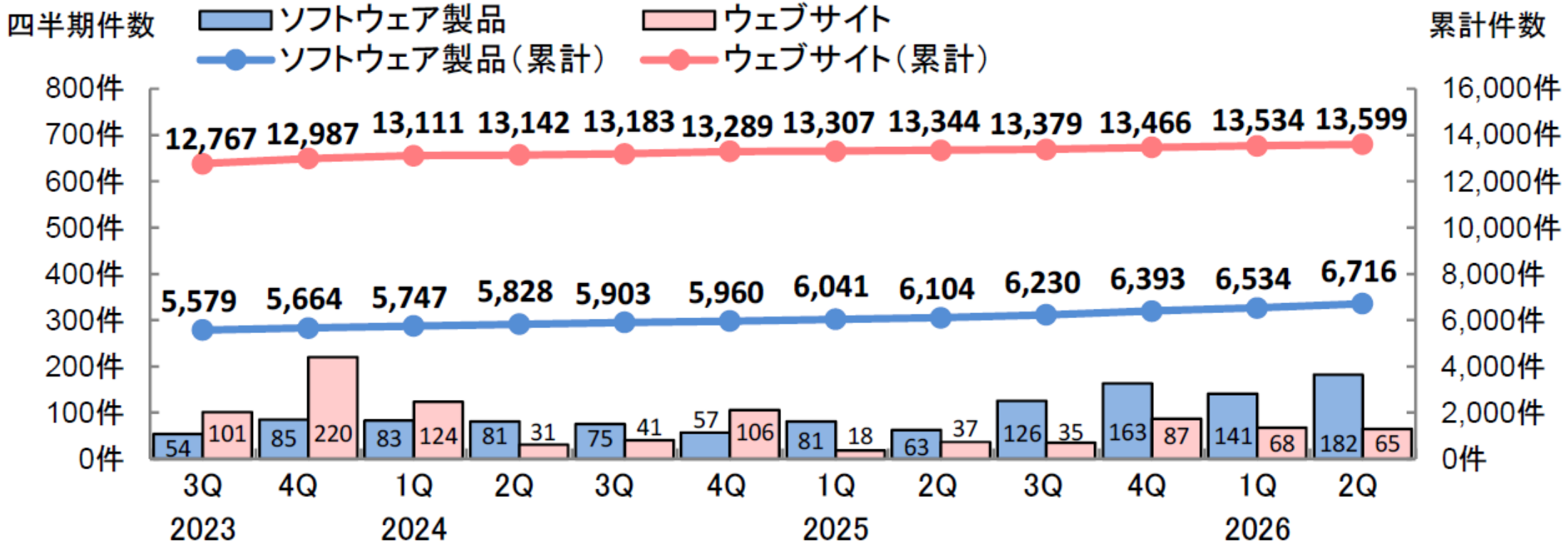


図 脆弱性の届出件数の四半期ごとの推移

出所：IPA「ソフトウェア等の脆弱性関連情報に関する届出状況[2026年第2四半期（4月～6月）]」
https://www.ipa.go.jp/security/reports/vuln/software/rcu1hd00000162jv-att/vuln_software_report_2026q2.pdf

大量パッチ時代の脆弱性対応：問題意識

■ 脆弱性情報の爆発的増加

- AIアシストによるコード解析ツールの普及とバグハンティングの自動化により、発見・報告されるCVEの数は爆発的増加
- 「脆弱性情報の洪水」により、手作業によるトリアージ（優先度判定）は限界に

■ 攻撃の高速化・自動化による「パッチ適用猶予時間」の消滅

- フロンティアAIは、脆弱性公表と同時にその内容をリバースエンジニアリングして動作可能な攻撃コードを自動生成可能

→　脆弱性が公表されてから攻撃コードが出回るまでの猶予期間：

【従来】数日～数週間：ユーザにパッチ適用の猶予

【現在】事実上消滅　：リアルタイムでの防御または先行的な対応が求められる

■ 開発・サプライチェーンにおけるAIコード生成のリスク

- 製品ベンダの開発現場でもAIコード生成アシスタントの利用が日常化
- 開発スピードを飛躍的に向上する一方、リスクも増大：
  - AIのミス（例：過去の脆弱なコードパターンを学習・再現、ライセンスや依存関係が不透明な OSS を製品内へ混入）
  - ソースコードの出自（Provenance）追跡が難化、製品ベンダが自社製品の構成や潜在的脆弱性を把握しきれないことも

■ 製品ベンダが直面するリソース・ケイパビリティの限界

- 国内製品ベンダにおいて、製品セキュリティを担う PSIRT の人材不足が深刻
- 脆弱性情報精査、自社製品への影響度調査、パッチ開発・検証、ユーザへの周知という一連のサイクルが破綻

大量パッチ時代の脆弱性対応：早期警戒Pは今後どうあるべきか？(私見)

■ 「脆弱性の嵐」との戦いの支援

- AIによる大量の深刻な脆弱性検出時代へ
  - ➡ 該当するソフトウェア製品/サービスの開発者は、同時に多くの脆弱性に対処しなければならない
  - ➡ 該当するソフトウェア製品/サービスのユーザは、複数の製品開発者から多数の脆弱性対策をほぼ同時期に通知される
    - → 適用に大規模なリソースが必要、24/365の重要サービスを止めざるを得ない可能性も
  - ➡ 膨大な脆弱性届出を人手で処理する限界、IPA・JPCERT/CCが機能不全に陥る可能性も

各セクタによるリスクベーストリアージへのシフトを支援

- 100点満点を強要しないコンセンサスづくり（優先すべき案件にリソースを集中）
- トリアージに資する判断根拠の提供
- 集中管理型からの脱却

■ 我が国に適した戦い方の提言

- 欧米で主流のソフトウェア製品が優先的に脆弱性検証の対象に ➡ 日本独自のソフトウェア製品の検証が遅れる可能性
- 多数の脆弱性対策の通知に対し、ユーザが自らに必要なトリアージを判断できない可能性

我が国のシステム市場・環境に即した対応を促進

- 国内市場におけるシェア・影響力、特性を考慮した脆弱性検証対象の選択
- システム構築・保守運用を担うSI事業者との連携

独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

Beyond Digital