

サポート終了を迎えたIEの歩みと Webブラウザの展望

キヤノンITソリューションズ株式会社
サイバーセキュリティラボ
マルウェアアナリスト
杉浦晃希

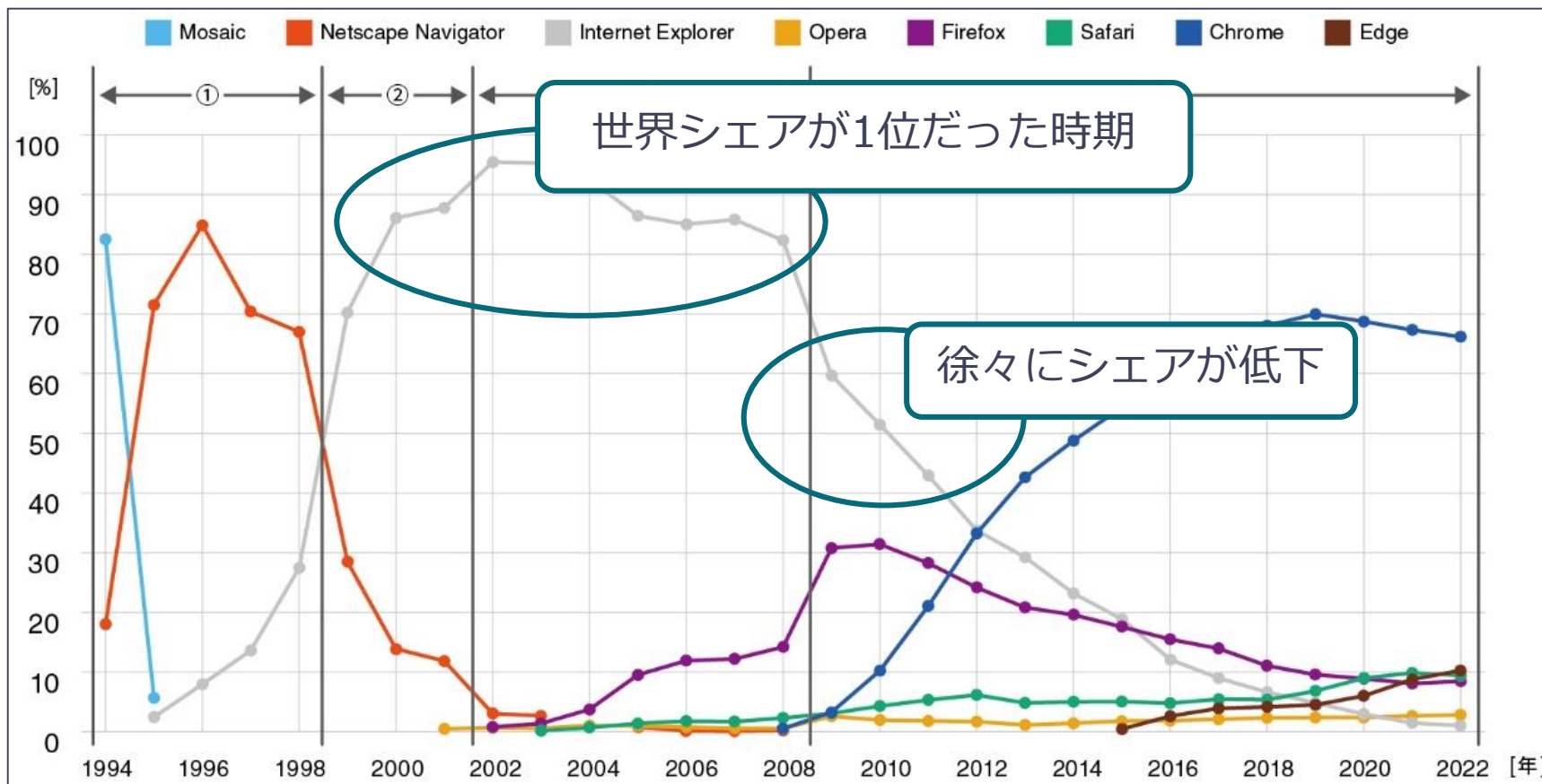
■ IE



- ✓ Microsoft社が開発したWebブラウザであるInternet Explorer(IE)
- ✓ 1994年に開発が開始、 Microsoft Plus! for Windows 95に同梱される形で1995年にリリース
- ✓ これまでにメジャーバージョンとしてInternet Explorer 1~11がリリース
- ✓ 2022年6月15日にサポートが終了

IEのこれまでの歩み

- ✓ 2000年代はWebブラウザの世界シェア1位
- ✓ 様々な要因によって、徐々にシェアが低下



主要なWebブラウザの世界シェア推移

※Georgia Institute of Technology、WebSideStory、OneStat.com、Statcounter GlobalStatsのデータから作成

Web標準（W3C）に準拠しなかった

- ✓ Webページの表示が崩れるケースが見られた（ユーザー視点）
- ✓ IE対応のためのコストがかかった（Web開発者視点）

ユーザビリティが低下した

- ✓ 独自機能を追加する際に動作が重くなることがあった

多くの脆弱性が発見された

- ✓ サイバー攻撃に悪用される機会が多かった

特徴

1. Microsoft社の独自機能に脆弱性が発見されることがあった
2. 利用ユーザーが多かったため、標的にされやすかった

ActiveX

IEの
独自機能

VBScript

Document
modes

1995件中1～100件表示中

ID ▼	タイトル
JVND-2021-004438	Internet Explorer 11 におけるリモートでコードを実行される脆弱性
JVND-2021-001526	Microsoft Internet Explorer 9 および 11 におけるメモリ破損の脆弱性
JVND-2021-001268	複数の Microsoft 製品におけるメモリ破損の脆弱性

脆弱性対策情報データベース | JVN iPedia

https://jvndb.jvn.jp/search/index.php?mode=_vulnerability_search_IA_VulnSearch&lang=ja&keyword=Internet+Explorer&useSynonym=1&vendor=2&product=27&datePublicFromYear=1998&datePublicFromMonth=01&datePublicToYear=2022&datePublicToMonth=10&dateLastPublishedFromYear=&dateLastPublishedFromMonth=&dateLastPublishedToYear=&dateLastPublishedToMonth=&cwe=&searchProductId=

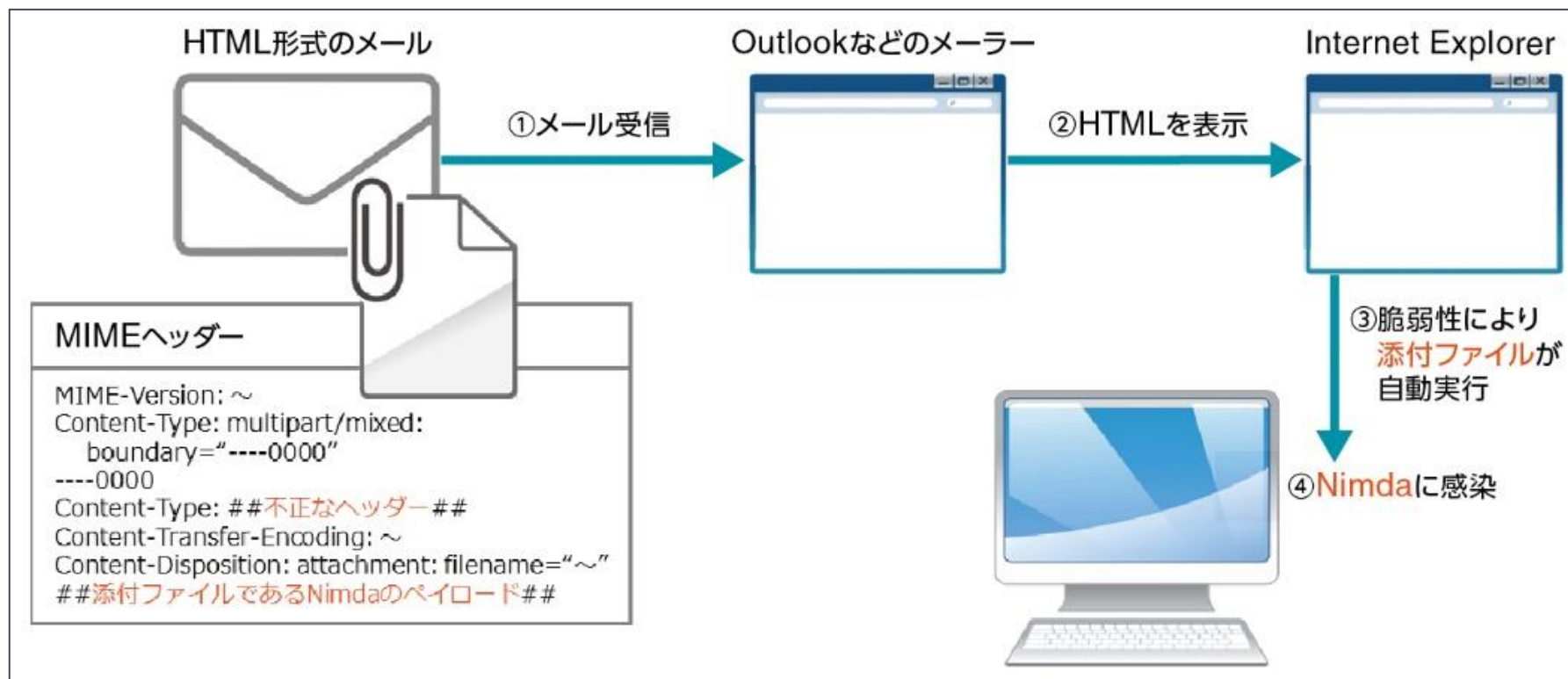
Nimda

- 2001年9月に確認されたワームの一種
- 多くの感染経路を備えたマルウェア
- 電子メール経由の感染手法では、CVE-2001-0154(※)の脆弱性を悪用

※IEのMIME処理不備による添付ファイル実行の脆弱性

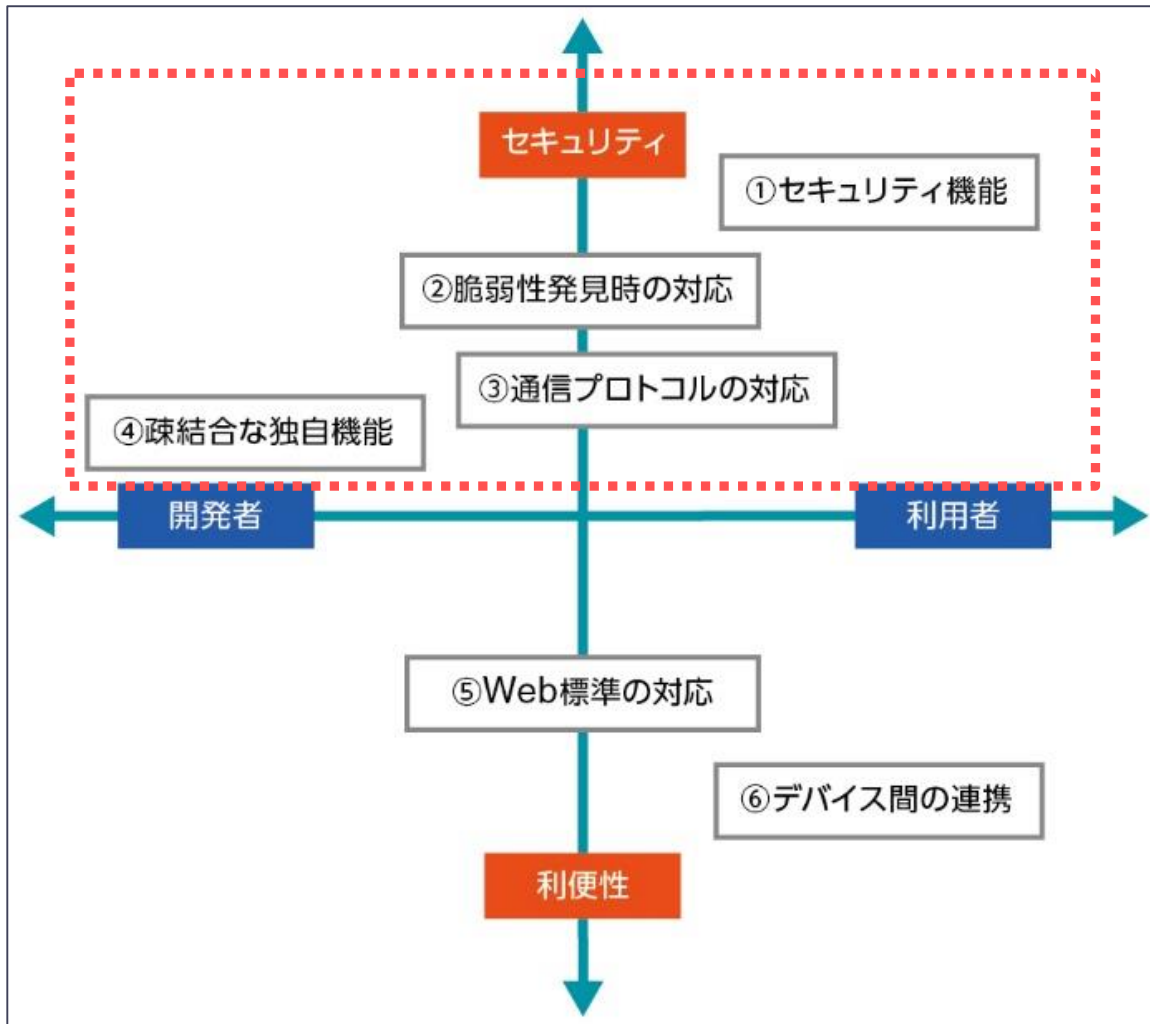
Nimdaの感染経路

- A. 電子メール
- B. ファイル共有
- C. Webブラウジング
- D. IISの脆弱性を悪用
- E. 別のマルウェアが作成したバックドア



電子メール経由によるNimdaの感染方法

今後のWebブラウザに求められる要素-セキュリティ 7



今後のWebブラウザに求められる要素

①セキュリティ機能

進化するサイバー攻撃に合わせて、必要なセキュリティ機能を追加

②脆弱性発見時の対応

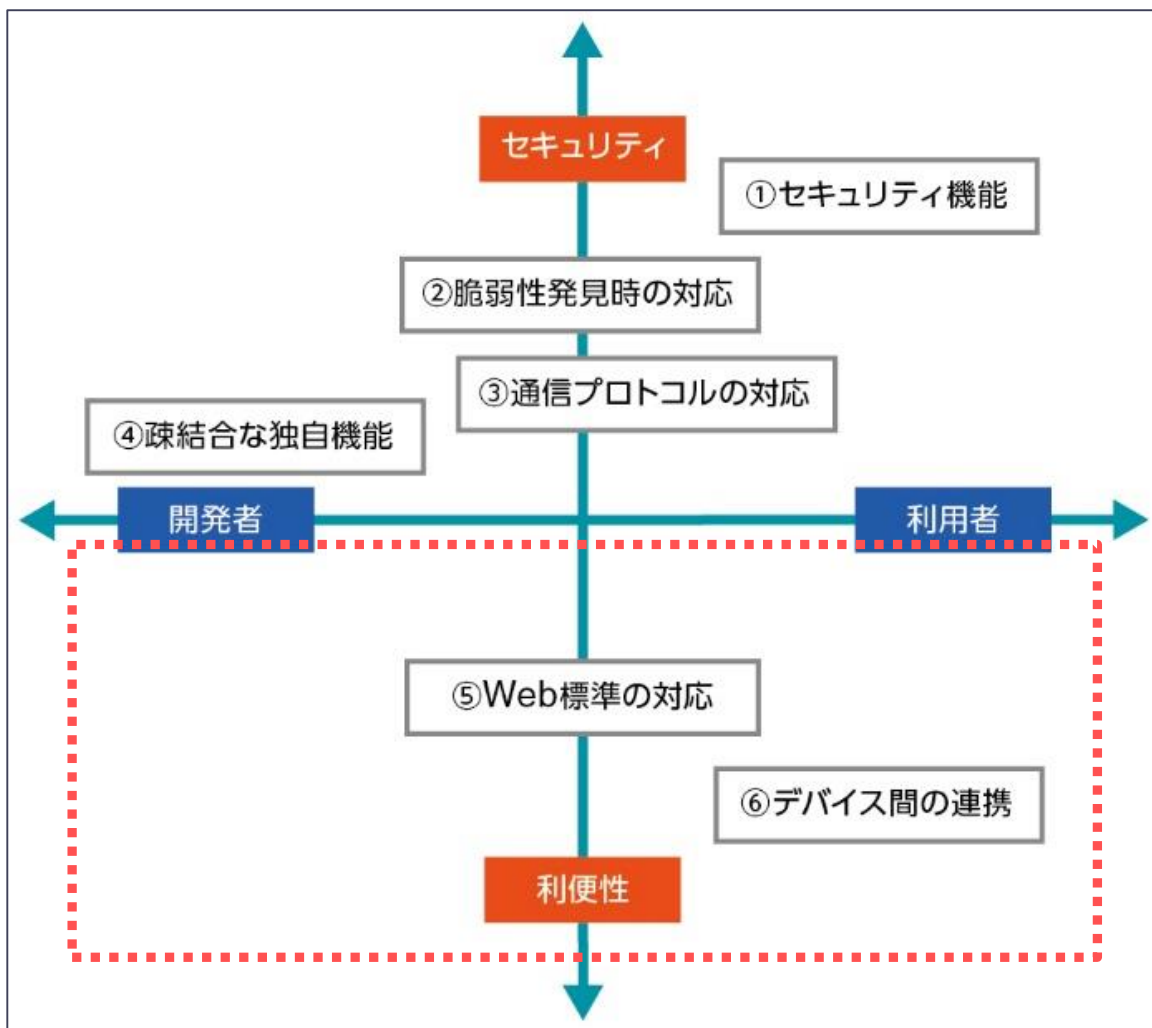
影響範囲や被害規模を抑え、個人や組織で継続利用しやすいブラウザ

③通信プロトコルの対応

最新の規格に素早く対応し、セキュリティやパフォーマンスを向上

④疎結合な独自機能

脆弱性や不具合が発見された際に、対応しやすいプログラム



今後のWebブラウザに求められる要素

⑤ Web標準の対応

W3Cに準拠した、使いやすく開発しやすいブラウザ

⑥ デバイス間の連携

デスクトップ端末やモバイル端末など、複数の端末で設定情報を共有

IEの継続利用

- ✓ サポート終了したソフトウェアは更新が行われないため**非推奨**

個人のWebブラウザ利用

- ✓ “今後のWebブラウザに求められる要素”を満たすブラウザを選択
- ✓ **アップデートを適用**し、サイバー攻撃に備える
- ✓ ブラウザのセキュリティ機能だけに頼らず、**別のセキュリティ製品と併用**