

## コラム記事

「自分たちは大丈夫」と考えていませんか？

ソフトを最新状態にせず放置しているサーバー・パソコン台数において、日本は世界3位、特にウィンドウズ搭載機器に関しては脆弱性の放置割合で日本は世界1位と不名誉な記録となっております。傾向として、中小企業での人材不足や予算不足等の理由によりバグや重大な欠陥が放置されている場合も多く「分かっているけど放置してしまう」企業が多いようです。

しっかりと対策を取るためのコストは、実際に被害が出た時のコストよりも少ないため、少しずつでも今できる対策を取っていく必要があると感じています。

そこで、ウィンドウズ搭載機器における脆弱性放置率についての、記事が掲載されておりましたのでご紹介いたします。



### 企業の老朽ソフト、世界で5割放置 サイバー攻撃懸念

(日経電子版 2022/1/22(火) 18:56 配信より引用)



セキュリティーセンターではサイバー攻撃を監視しているが… (日経電子版より引用)

企業がホームページ運営などに使うサーバーや基幹パソコンを調べたところ、サイバー攻撃の恐れのある古いソフトが世界の機器の5割で放置されていることが分かった。日本は米マイクロソフトの基本ソフト「ウィンドウズ」搭載機器の3割で脆弱性が見つかった。サイバー攻撃で情報が漏洩すると企業は4月施行の改正個人情報保護法で報告を求められる。海外で罰金を科される恐れもあり対策が急務だ。

ITソフトを手掛ける米タニウムの協力を得て検索システム「SHODAN」の公開情報を使い、2021年12月に調査した。

対象はインターネットに接続し、マイクロソフトの「ウィンドウズ」とApache（アパッチ）ソフトウェア財団のウェブサーバーソフト「Apache」を使ってホームページなどを運営する世界のサーバー・パソコン約2577万台。

サイバー攻撃を受ける恐れのあるソフトの深刻な脆弱性12項目について調べた。ホームページなどを運営していない個人の

パソコンは含まない。

### 世界の脆弱性の総数で日本は3位

1	米国	351万台
2	ドイツ	93
3	日本	88
4	中国	67
5	フランス	57

(注)ウィンドウズとApacheの対策不備12項目

### ウィンドウズの脆弱性放置の地域別比率では首位

1	日本	30%
2	台湾	24
3	ロシア	9
4	米国	7
	その他	30

(注)乗っ取りの標的となるSMBv3の対策不備 (日経電子版より引用)

12項目の脆弱性のうち1項目以上でソフトを最新状態に更新せず放置しているサーバー・パソコンは、世界で1268万台と調査対象の5割を占めた。所在国別にみると、米国が351万台と首位だった。日本は約88万台とドイツ(93万台)に次いで3位だった。

米国の台数が多いのは調査対象となった機器が多いためだ。各国の機器総数に対する脆弱性の見つかった比率をみると、日本は45%と米国(43%)やドイツ(42%)を上回る。

日本はウィンドウズを搭載するサーバー・パソコンで脆弱性の放置割合が高い。

ウィンドウズで脆弱性が見つかったのは世界で約5万6300台ある。全体に占める割合は少ないが、ウィンドウズは他のソフトよりも企業全体を動かす重要なシステムに使われている比率が高く、サイバー攻撃された場合の深刻度が大きい。

各国のウィンドウズの所有機器数に対する脆弱性比率でも日本は30%と最多だった。主に中小企業でバグや重大な欠陥が放置されているとみられる。

危険性が高いものの一つが、ウィンドウズの通信機能「SMBv3」の脆弱性だ。身代金(ランサム)要求ウエア「WannaCry(ワナクライ)」などの不正ソフトの足がかりとなる。ワナクライは17年に大流行し、日立製作所やJR東日本が被害を受けた。

日本で脆弱性が見つかったのは約7300台と世界全体の30%を占め、台湾、ロシア、米国を上回り首位だった。

マイクロソフトなどはこうした脆弱性を修正するソフトを配布し更新するよう呼びかけている。だが人材不足や予算不足などを背景に、放置されている例が多い。日本マイクロソフトは「システムを確認したうえで、速やかに修正プログラムを適用してほしい」としている。

サイバー攻撃は急増している。米調査会社サイバーセキュリティ・ベンチャーズによると、ランサムウエアによる世界の被害額は21年に約200億ドル(約2兆2600億円)と15年の約60倍に増え、31年には2650億ドル(約30兆円)に達すると予測する。

最近ではホームページやネットサービス運営のログ管理などに使われる「Apache Log4j(アパッチ ログフォージェイ)」と呼ばれる機能で重大な欠陥が見つかり、問題となった。

サイバー攻撃を受けて情報が漏洩した際の経営リスクは大きくなっている。米マリオット・インターナショナルや英ブリテッシュ・エアウェイズなどは欧州の一般データ保護規則(GDPR)で100億円を超える制裁金(後に減額)を科された。

日本でも 4 月施行の改正個人情報保護法で報告義務が課される。企業も取引先の情報管理を重視するようになっており、漏洩すれば取引を打ち切られる恐れがある。

企業のサイバーセキュリティ対策は遅れている。IDC ジャパンによると、日本企業の約 56%が IT 投資でセキュリティ対策予算を設定していない。

あるエネルギー関連企業のセキュリティ担当者は「経営者から重視されず、予算が限られている」と話す。

日本ブルーポイントの増田幸美氏は「ハッカーの攻撃では超高度な手法よりも古典的な手法が根強く使われている」と指摘する。偽メールからウイルスをダウンロードさせたり、古いソフトのバグを狙ったりすることが多い。

米調査会社ポネモン・インスティテュートによると、サイバー攻撃の予防措置をとることで、実際に被害が出たときよりもコストを 85%減らせるという。



世界の先進国と比較しても日本のセキュリティ対策は遅れていると言われています。

その中でも脆弱性を理解していても、人員や予算の関係で止む無く放置されている企業も多いのではないかと感じています。

しかしながら、サイバー攻撃被害は日本のみならず世界でも日々報告されているため、サイバーセキュリティに対する優先順位を検討し、出来るところから対策を進めていくことが必要不可欠な時代になってきていると考えております。