2020 年 10 月 23 日(金)

報道関係者各位

厳しい条件のもとでも高い意識で脆弱性管理に取り組む「一人情シス」たち ～ 日本企業の脆弱性管理実態探る５００名調査実施

株式会社ブロードバンドセキュリティ
株式会社イード

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 CEO：持塚 朗、以下 BBSec)は、株式会社イード(本社：東京都新宿区、代表取締役：宮川 洋、以下 イード)と共同で、企業の脆弱性管理に関する実態調査を行いました。

「脆弱性（ぜいじゃくせい)」とは、サーバや Web アプリケーション、ネットワーク機器などに、さまざまな理由で発生したプログラム上の欠陥のことで「セキュリティホール」とも呼ばれます。脆弱性を悪用すれば悪意のある第三者がサイバー攻撃を行うことが可能となるため、脆弱性に関する情報収集を行い、見つかった場合は、脆弱性をふさぐ「パッチ」と呼ばれる修正プログラムを適用する必要があります。

本調査は、勤務先で「脆弱性管理」「パッチ管理」の実施に関わる、企業の情報システム部門や総務担当者等５０７名を対象にアンケートを行い、ソフトウェアの脆弱性（セキュリティホール）を日頃どのように管理しているかを明らかにしたもので、これまで国内で、一般に公表された同種の調査はほとんど存在していません。

■■調査概要

調査手法：アンケートモニターを利用した、インターネット調査
調査対象者：企業や組織内の「脆弱性管理」「パッチ管理」の実施担当者
有効回答数：507
調査期間：2020 年 8 月 6 日（木）～13 日（木）

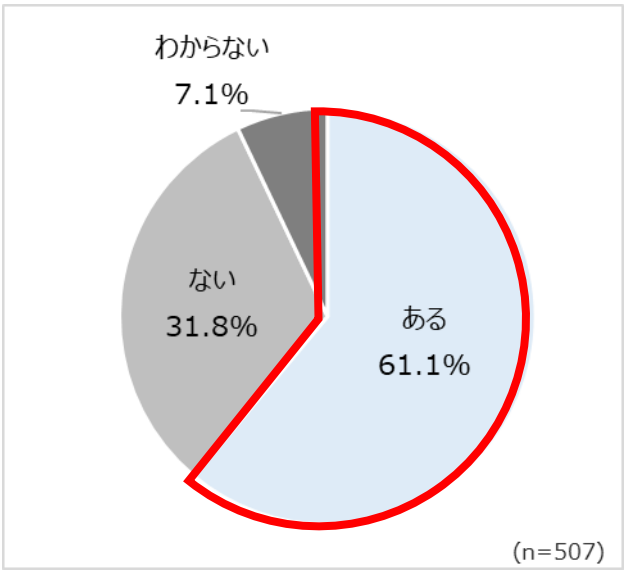
■■本調査の主なトピック

本調査は、サーバやネットワーク機器、自動アップデートが行われないソフトウェア、自社開発のソフトウェアや Web アプリケーション等を対象として実施しました。ソフトウェアベンダによるアップデートが自動で行われる Microsoft Windows や Adobe 製品等は対象としていません。

■トピック１　６割が未適用パッチ有、原因は不充分な資産管理とテスト環境の不備

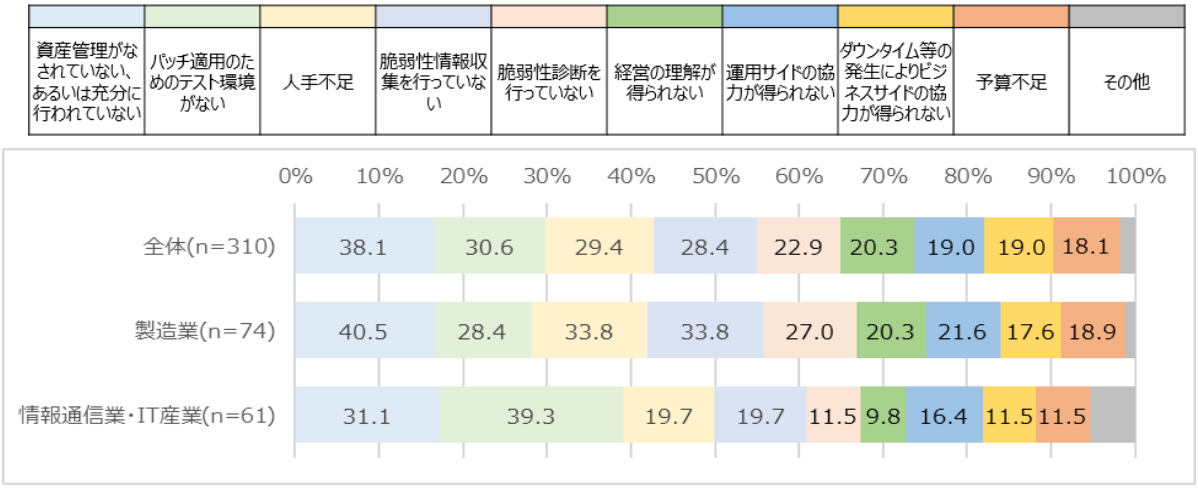
「自動アップデートが行われないソフトウェア、自社開発のソフトウェアや Web アプリケーション等に未適用のパッチはありますか」という質問に対して、61.1 %が、未適用のパッチがあると回答しました。

未適用のパッチ有無



未適用のパッチがある理由として「資産管理がなされていない、充分に行われていない(38.1 %)」がもっと高く、「テスト環境がない(30.6 %)」「人手不足(29.4 %)」が続きました。また「経営の理解が得られない（20.3 %)」「運用サイドの協力が得られない（19.0 %)」などの根本的な組織的理解の不在も明らかになりました。

業種×未適用パッチがある理由

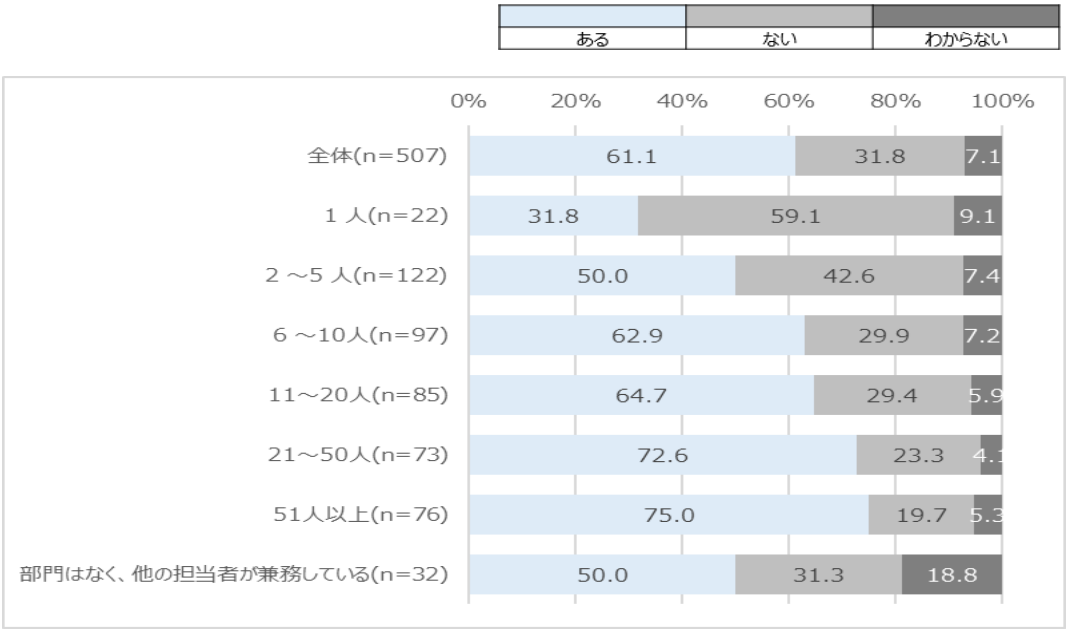


■トピック２　未適用パッチは情報システム部門の人数に比例して存在

「一人情シス」という情報システム部門の人材不足を示す言葉がありますが、情報システム部門の人数が確保されれば脆弱性管理は充分に行われるのでしょうか。調査はむしろ反対の結果となりました。

情報システム部門が 1 名の場合、未適用パッチ有りは 31.8 %に対して、情報システム部門の人数が 51 名以上の場合、未適用パッチ有りは 75.0 %となっています。

情報システム部門の人数×未適用のパッチ有無



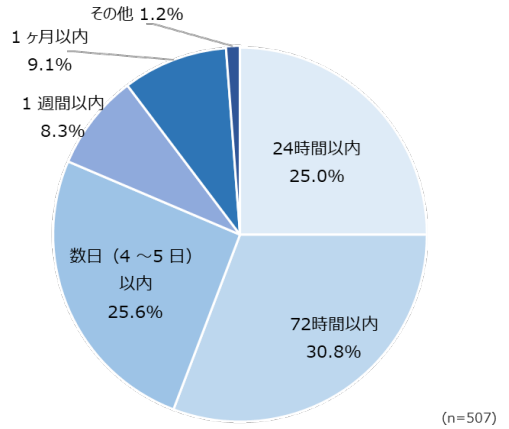
情報システム部門の人数は、組織規模に比例し、規模が大きいほど運用システム数も多くなり、脆弱性を抱えたままのシステムが多くなる傾向が見て取れます。

■トピック３　パッチ情報入手とパッチ適用はいずれも７２時間以内が半数

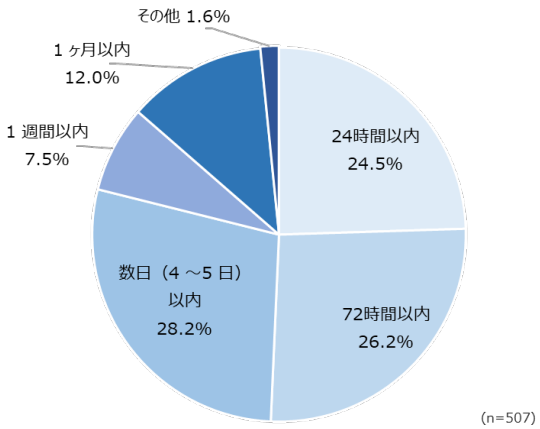
ソフトウェアや機器の脆弱性は、提供ベンダやセキュリティ企業、セキュリティ機関などによって、脆弱性の修正プログラムであるパッチ情報とともに公表されます。

パッチ情報が公開されてから情報を入手するまで、そして入手した情報をもとに検証を行いそれを適用するまでの時間に関する質問に対しては、いずれも約半数が 72 時間以内と回答しました。

パッチ情報が公開されてから入手するまでの平均時間



パッチ情報を入手してから適用するまでの平均時間

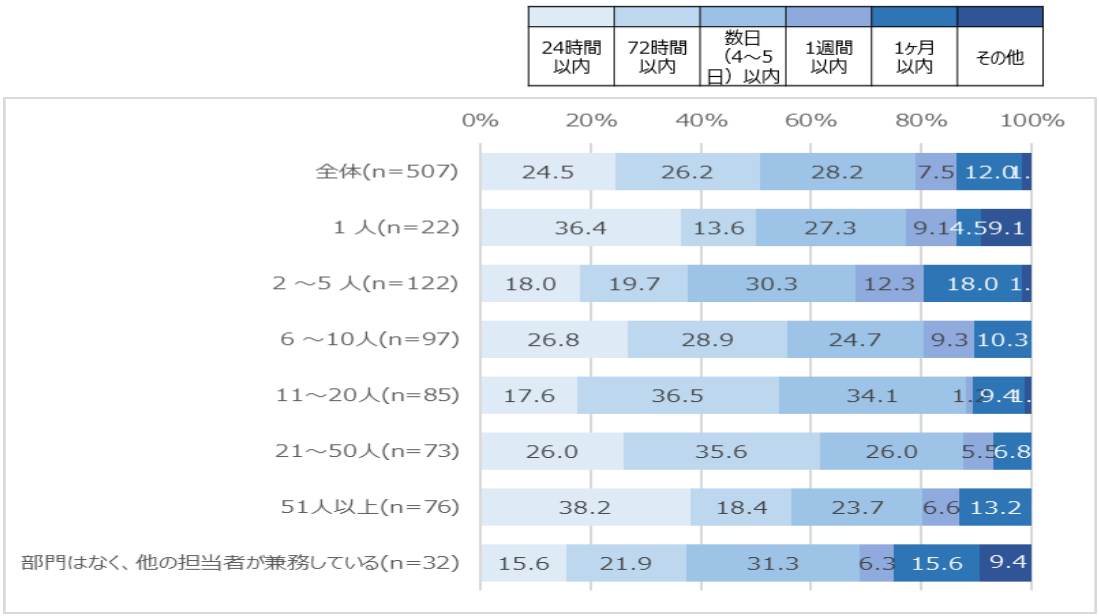


情報システム担当者は、不充分な資産管理やテスト環境の未整備、人手不足、非協力的な現業部門、経営の無理解など、いちじるしく厳しい条件のもとにありながら、多忙な通常業務をこなす中、ある日突然飛び込んでくる脆弱性とパッチ適用に対して、極めて迅速に対応している実態が明らかになりました。

パッチ情報の入手から適用までの時間を、情報システム部門の人数規模で比較したデータはとりわけ目を引く結果となりました。最も短い「入手から適用まで 24 時間以内」と回答した比率は、情報システム部門が 1 名の場合 36.4 %、情報システム部門が 51 名の場合 38.2 %と、その差 2 %未満という、ほぼ変わらない数値を示しています。

一人情シスが大企業の情シスと何らの遜色がない水準の管理を行っていることを示すこの結果は、脆弱性管理ひいてはセキュリティ管理に携わる技術者の、責任感と矜持の高さを示す結果であるとイードと BBSec は考えます。

情報システム部門の人数×
パッチ情報を入手してから適用するまでの平均時間



■トピック４　脆弱性管理の最適化のために約８割の企業が脆弱性診断サービスを利用

ベンダやセキュリティ機関等によって脆弱性公表がなされない、自社開発のシステムやWeb アプリケーションなどの脆弱性を検知する目的で脆弱性診断サービスを実施したことがあるという回答は 76.9 %となりました。ペネトレーションテスト（ 58.6 %）やソースコード診断（ 55.8 %）の利用も半数を超えており、DX を迎えようとする時代に、企業活動において専門セキュリティサービスを活用することが一般的になっていることを示しています。

■■本調査結果の提供について

本調査の調査結果全文は 10 月 28 日以降、下記の URL からダウンロードできます。

●「脆弱性管理に関するアンケート インターネット調査レポート」2020 年

https://www.sqat.jp/

（株式会社ブロードバンドセキュリティ　セキュリティ・サービス本部サイト「SQAT.jp」）

■■本調査結果のウェビナーについて

10 月 28 日　10:30-11:30

500 人に聞きました　「あなたの会社の脆弱性管理・パッチ管理は大丈夫ですか？」

株式会社ブロードバンドセキュリティ　セキュリティサービス本部

セキュリティ情報サービス部部長　田澤千絵

https://www.cocripo.co.jp/webinar/detail/9e09fd6b-c28b-4bc6-bf90-3066a360a516

10 月 30 日　14:00-15:00

脆弱性管理、それでいいの？500 人調査から見えること

合同会社エルプラス 代表社員　杉浦 隆幸 氏

株式会社ブロードバンドセキュリティ セキュリティサービス本部 本部長　齊藤 義人

https://www.cocripo.co.jp/webinar/detail/0ad70a4d-3578-48cf-bdf9-bf2f96c2ad86

■■本リリースに関するお問合せ/取材等の窓口

株式会社ブロードバンドセキュリティ
管理本部　経営企画部　コーポレート・コミュニケーション課　高橋・内海
sqat-inq@bbsec.co.jp

〒160 - 0023
新宿区西新宿 8-5-1 野村不動産西新宿共同ビル 4F
TEL: 03-5338-7430