SQAT® SECURITY REPORT

2020-2021年 秋冬号

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
東京都新宿区西新宿 8-5-1 野村不動産西新宿共同ビル 4F
TEL：03-5338-7417　FAX：03-5338-7435
https://www.bbsec.co.jp/

知る・守る
続ける

BBSec は内閣サイバーセキュリティセンターの
「サイバーセキュリティ普及啓発」に賛同しています

はじめに

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

本レポートは、株式会社ブロードバンドセキュリティ（以下、BBSec）の脆弱性診断サービス「SQAT®」における 2020 年上半期（1 月～ 6 月）の膨大な診断結果からデータを抽出し、集約したものを、当社のエンジニアらの感性も交えてアウトプットしたレポートです。主にサイバーセキュリティのトレンドや展望についてお楽しみいただくことができる内容となっております。

新型コロナウイルスが、世界中にさまざまな影響を及ぼしています。その影響範囲や社会情勢の大きな変化を予想できた人はあまりいないでしょう。想定外の事態には、その場で対応するしかありません。本レポートをご覧の方の大半が、私生活や仕事で、「変化を余儀なくされた」ことに多少はさいなまれたことと思います。しかしながら、「変化を余儀なくされた」を、言い換えることはできませんか？「利点があることはわかっていたが、これまで先延ばしにし続けてきたことを、実行するときがきた」と。そのすべてが悪いことではないはずです。

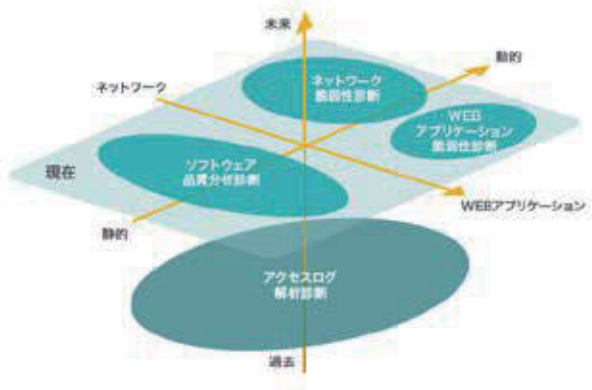
情報セキュリティの未来を「創造」するためには、斬新な発想はもちろん、統計データ等の数値や、現場からのさまざまな声から導き出される、「想像」が必要です。ただし、数字や現場からの声からうかがえる「現実」は、ときとして受け入れがたいものです。技術的な問題にとどまらず、組織や経営からの IT システムや IT 部門への理解に起因する問題も垣間見えることもあるからです。それを受け入れ、改善することで、初めて斬新な発想が実現されます。巻頭企画では、多様な規模の企業に勤務する情報システム管理担当者を対象とした Web アンケートの調査結果から、脆弱性管理やパッチ管理の現状を浮き彫りにします。

我々人類は、弱い生物であることを自覚しています。だからこそ、太古よりさまざまな技術を駆使して便利な道具や機械を作る、システムを構築するなどし、豊かな生活を確保すると同時に安全な社会を築いてきました。サイバー攻撃をするのは人間です。攻撃するからには、当然わかりきっている、「人は弱い生物だ」という点を突いてくることがあります。注目テーマとして、人をターゲットにしたサイバー攻撃、「ソーシャル・エンジニアリング攻撃」に焦点を当てました。

本レポートが、読者の皆様のセキュリティ対策における有益な情報としてご活用いただけることを願ってやみません。それこそが「便利で安全なネットワーク社会を創造する」をモットーに掲げる BBSec の使命であると考えております。

SQAT®（Software Quality Analysis Team）とは
～スペシャリスト集団が組織の脆弱性対策をトータルに支援～

「SQAT®」は、BBSec がご提供する脆弱性診断サービスです。エンジニア、コンサルタント、ホワイトハッカー等から編成された精鋭チームが、あらゆる側面から網羅的な診断を実施。スペシャリストのノウハウを結集して組織の情報システム強化をお手伝いします。お客様は金融機関・インターネット事業者などの民間企業から、官公庁をはじめとする公共機関まで幅広く、これまでに延べ 5,300 組織、31,500 を超えるシステムで利用されています。



CONTENTS

巻頭企画

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?」

SQAT® Security Report 編集部

当社では 2020 年 8 月に企業の情報システム管理担当者 500 人を対象に脆弱性管理やパッチ管理の現状を Web 調査した。「今時なぜそんなテーマ?」と思われる読者もいるかもしれない。しかし、当社の脆弱性診断の結果でも、「バージョン・パッチ管理に関する問題」を抱えるシステムが 25% を超える割合で存在している。Web アプリケーション独自、ソースコード独自の脆弱性よりもはるかにプラットフォームの OS やソフトウェアの脆弱性が大量に検出され、その数は一向に減らないどころかむしろ増加傾向にある。その背景をまず明らかにし、その原因を共有することが、これからの IT システムや情報セキュリティを考えるヒントになると考えた。この調査結果について、本稿では調査の概要と結果の速報をお知らせしたい。

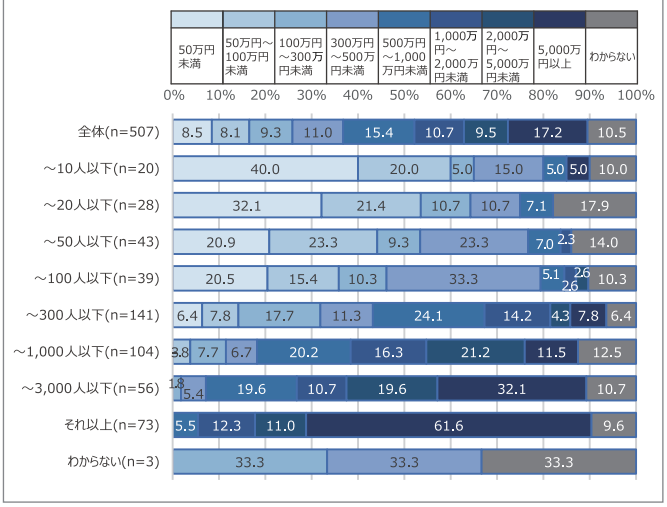
調査概要

今回の調査は多様な規模の企業にお勤めの 507 人の方に匿名にてご協力いただいた。まずはご協力いただいた方々に感謝申し上げたい。

調査目的	国内企業の脆弱性管理方法に対する実態を調査し、把握する。
調査対象	お勤め先で「脆弱性管理」「パッチ管理」の実施に関わっている方
調査期間	2020 年 8 月 6 日 ~13 日
調査方法	Web アンケート調査
回収結果	有効回答数 507 件

ご回答いただいた方々の勤務先の会社規模も 10 人以下から 3000 人以上まで幅広く、情報システム部門の人数も 1 人から 50 人以上まで多様であった。情報セキュリティ対策の予算も年間 50 万円未満から 5000 万円以上と幅広かったが、CSIRT（Computer Security Incident Response Team：セキュリティインシデントに対応するための専門チーム）がある企業が半数以上、PCI DSS（Payment Card Industry Data Security Standard：クレジットカード業界の国際的なセキュリティ基準）の認証を受けている企業も 4 割程度と、情報セキュリティ対策に一定程度以上の予算を割いている企業が多いことが分かった。特に会社規模が 100 人を超える規模から、情報セキュリティ対策にかける金額がぐっと増えていることがわかる。

図 1　回答者の勤務先の会社規模（縦）と情報セキュリティ対策年間予算（横）



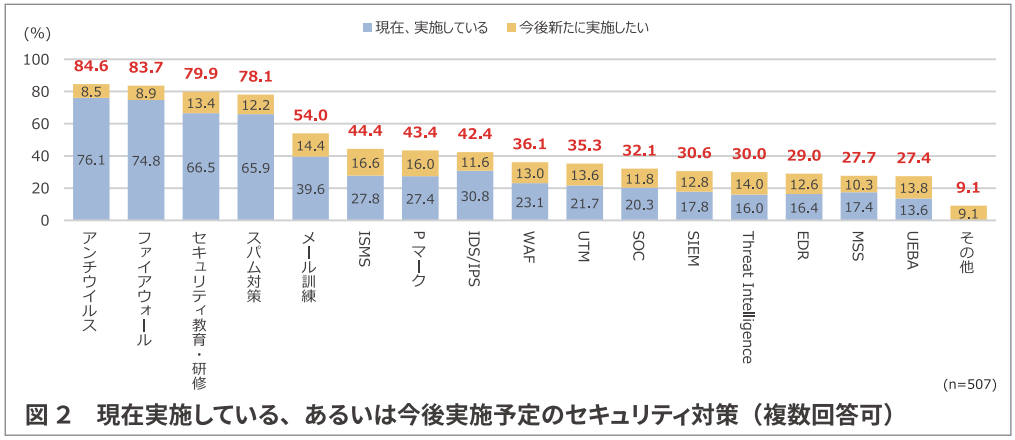


図 2　現在実施している、あるいは今後実施予定のセキュリティ対策（複数回答可）

各企業が実施している情報セキュリティ対策の主要なものとしてはアンチウイルス、ファイアウォール、セキュリティ教育・研修、スパム対策が主流となっている。

未適用のパッチがある背景は

一定規模以上の企業では情報セキュリティ対策に予算を割くなどある程度、情報セキュリティの重要性が認知されている一方、クライアント PC を除く IT 資産（ネットワーク機器やサーバ、自動アップデートが行われないソフトウェアや Web アプリケーションなど）について未適用のパッチが存在するかどうか聞いてみたところ、未適用のパッチがあるという回答が 61.1%となった。

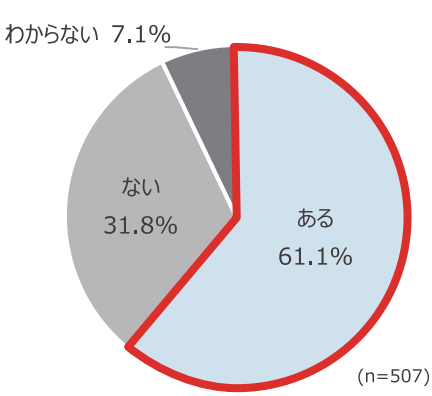


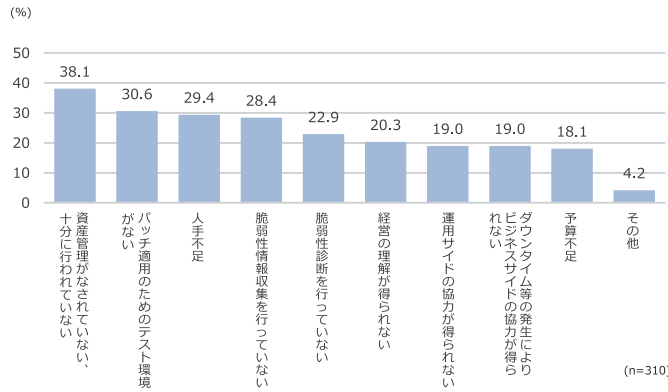
図 3　未適用のパッチの有無

さらに、「未適用パッチがある」原因を確認したところ、主に以下の 3 つに分類できることが分かった。

1) 未適用パッチがあることが発見できないこと（資産管理・脆弱性情報収集・脆弱性診断の問題）
2) パッチの適用に必要な環境が十分でないこと（テスト環境・人手・予算の不足）
3) パッチの適用のために必要となる周囲の理解が不十分なこと（経営・運用・ビジネスサイドの理解・協力）

これらを企業規模別に集計したところ、人手不足は情報システム部門の人数に関わりのない問題であることが見えてきた。むしろ「人手不足」と回答している割合が、情報システム部門の人数 51 名以上の回答群で最も高い（担当者 1 名の回答群を除く）。システム部門の人数は運用しているシステム全体の規模と比例すると考えられることから、システムの規模が大きくなるにつれてパッチが適用されない、つまりは脆弱性がそのままになっている資産が社内のどこかにある可能性も高くなるという推測が可能となる。

図 4　未適用パッチがある原因（複数回答可）



また同じように「運用サイドの協力が得られない」「ダウンタイム等の発生によりビジネスサイトの理解が得られない」との回答も情報システム部門の規模と関わりなく存在する問題であることも明らかになった。規模の大きなシステムになると BCP などの関連から複雑な冗長構成となっていることが多く、フェイルオーバーや切り戻しなどの通常運用以外の手順が発生することから運用サイドの同意を得られないケースが多いことも関係しているかもしれない。また、OS 等の場合にはアプリケーションとの互換性の問題から運用側にパッチの適用を断られるケースもあるだろう。さらに、アップデートが発生する箇所によっては手順が異なってくることも想定され、深刻度が低いと判断された脆弱性はそのままにするという判断にもつながっているのではないかと考えられる。

図 5　情報システム部門の人数と未適用パッチがある理由（複数回答可）