SQAT®
SECURITY REPORT

2021年 春夏号

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 年下半期（7 月～ 12 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。

読者のみなさまの中には、新型コロナウイルスを想定した「ニューノーマル」に慣れてきた方もいらっしゃると思います。そして、感染者の推移に不安を感じながらも、仕事や生活必需品を購入するために、ある程度覚悟の上で外出する機会も増えているのではないでしょうか。それでも、「新型コロナウイルスの蔓延」というのは、人類史上記憶にも記録にも残り、おそらく後世に語り継がれていく出来事です。同時に、テクノロジーの変革についても、まさに今その時を迎えています。

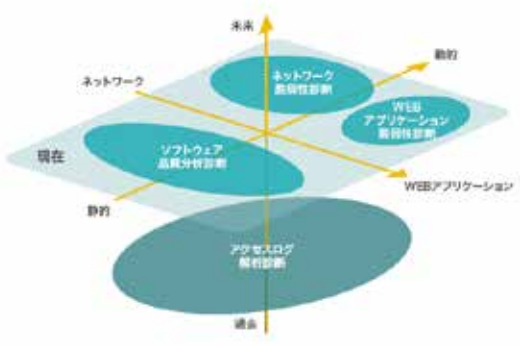
新型コロナウイルスの蔓延により、リモートワークの推進などビジネス環境にも変化がもたらされた事態は多くの企業や組織が経験したことでしょう。後に振り返ったとき、語られるエピソードは次のいずれになるでしょうか。「急速な変化が混乱を呼び、セキュリティを整備しきれなかった企業から情報資産が漏洩してしまい、業績不振に陥ってしまった」、「変化に柔軟に対応し、適切なセキュリティを整備できた企業が信頼され、情報セキュリティを重要視する様相が一層強まった」。巻頭企画では、リモートワークの普及など、新型コロナウイルスの影響で変化する環境下で浮上しているセキュリティの問題や脆弱性対策について焦点を当てました。

さらに注目テーマでは、「ホワイトハッカー」と呼ばれる人々がサイバーセキュリティに与えた影響や恩恵に着目しております。コンピュータやインターネット、モバイル機器などの普及に始まり、現在も情報技術の高度化は留まるところを知りません。現代社会において、情報技術を駆使してビジネスをすることは当たり前で、ビジネスで動く莫大な資金や情報資産を守る技術も、当然高度なものでないといけません。守る技術が高度でなければならない理由のひとつには、金銭や情報を狙ったサイバー攻撃の高度化が挙げられます。高度なサイバー攻撃に対抗するためには、高い技術力をもち、サイバー攻撃をする側の視点で対策や防御策を提案できるスペシャリストも必要です。このような、高い技術力でセキュリティを担う「ホワイトハッカー」たちの偉業を紹介します。

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。

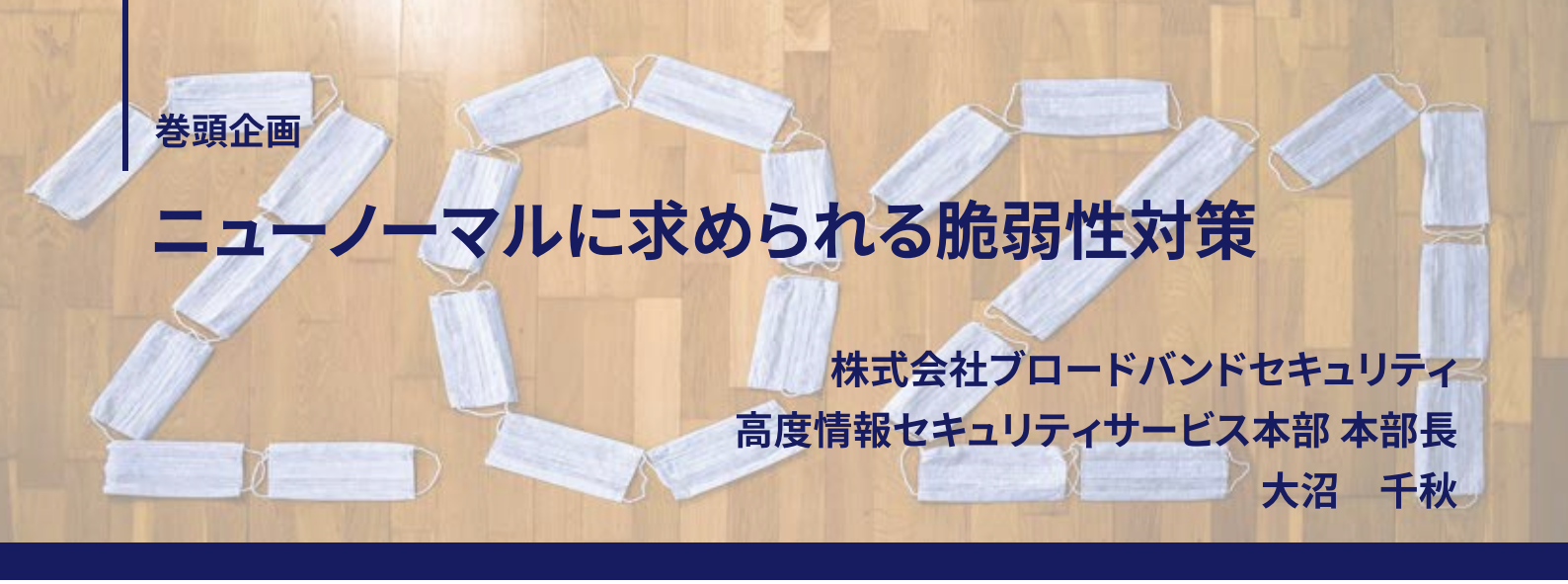
SQAT®（Software Quality Analysis Team）とは
～スペシャリスト集団が組織の脆弱性対策をトータルに支援～

「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 5,810 組織、35,000 を超えるシステムで利用されています。



CONTENTS

※本レポートは、当社セキュリティサービス本部のホームページ
「SQAT®.jp（URL：https://www.sqat.jp/）」
https://www.sqat.jp/sqat-securityreport/ からダウンロード可能です。



巻頭企画

ニューノーマルに求められる脆弱性対策

株式会社ブロードバンドセキュリティ
高度情報セキュリティサービス本部 本部長
大沼　千秋

去る 2020 年は、新型コロナウイルス感染症（COVID-19）のまさに世界規模なパンデミックにより、我々の生活ばかりでなくビジネスをも大きく変革させた一年だった。中でもテレワーク、リモートワークといった遠隔による勤務形態の整備は、従来様々な理由から普及が伸び悩んでいたが、ここ一年ほどの間で加速度的に普及しつつある。また、ビジネスにおける IT 環境も、クラウドシフトが一気に進行している。

従来のオンプレミス型からクラウド型へのシステム構築・運用環境の移行は、様々な企業の IT 戦略において、優先度の高い課題といえるだろう。そして、テレワーク、クラウドシフトが進んでいく中で、新たなセキュリティ上の問題が顕在化してきていることも事実だ。特に、急ピッチでこれらの環境を整備し、運用開始しているケースでは、以前よりもサイバーセキュリティ脅威および危険性は増大しているといっても過言ではない。本稿では、アフターコロナにおけるニューノーマルを見据えた企業における脆弱性対策に焦点を当て、どういったことを推進していくことが必要か解説していきたい。

テレワークとクラウドシフトに伴う脅威

企業のネットワークや OA システムといった IT インフラには、既に様々なセキュリティ対策が講じられているものと思われる。このセキュリティ対策の大原則は、インターネットとの境界を防御するという考え方に基づいており、ファイアウォールによるアクセス制御、攻撃検知のための侵入検知・防御システム（IDS・IPS）、DMZ（DeMilitarized Zone：非武装地帯）を用いた公開システムの区分、安全な Web 閲覧のための Web プロキシ、マルウェア対策ツール、EDR（Endpoint Detection and Response）による監視、といった対策を組み合わせることによるセキュリティの確保を意味する。

ところが、昨今のテレワーク、クラウドシフト（図1、図2参照）で在宅による業務環境の提供が不可欠となったことにより、社内の環境は一定のセキュリティが確保されているので安全である、という前提が崩れてきている。本来であればインターネットから接続できない各種業務システムへのアクセス許可や、業務における各種情報を共有するためのクラウドストレージサービスの利用、営業活動における情報管理のための CRM（Customer Relationship Management：顧客管理システム）の導入、グループウェア等に代表される SaaS 型クラウドサービスの活用等といった具合に、業務システムが様々な領域へと進出し、多様化してきていることから（次ページ図3）、セキュリティ対策としては一箇所だけを守ってい

図 1　東京都内企業（従業員 30人以上）のテレワーク導入率

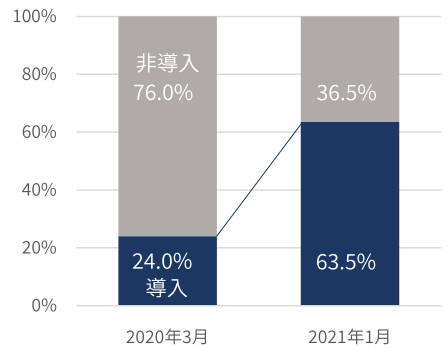


図 2　国内クラウド市場　実績と予測

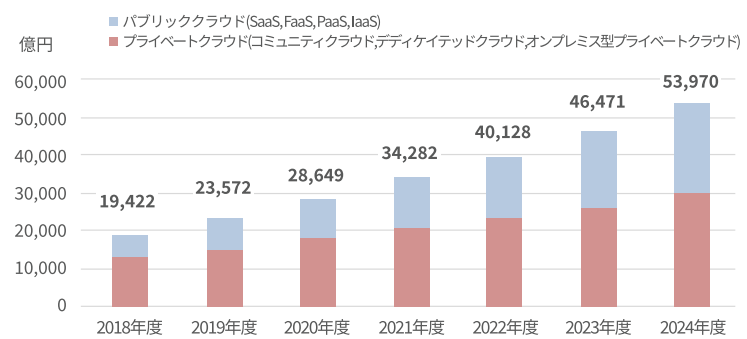
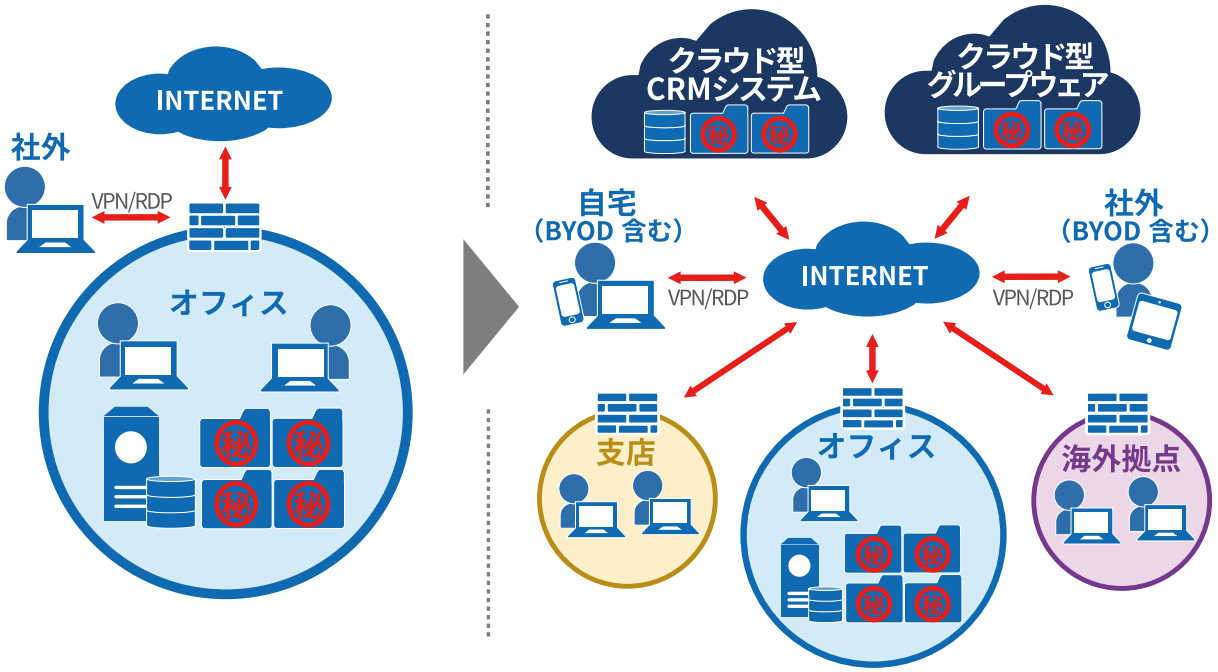


図3　ビジネス IT 環境の変化



れば安全である、という常識は既に覆っていると考えて間違いない。

例えば、テレワーク導入を急ピッチで進めている中で、暫定的に VPN により社内ネットワークへの接続を許容するケースは、よく耳にする話だ。しかし、これはいわば企業が提供する公式のバックドアを開けているようなものであり、サイバー攻撃者に VPN が突破されてしまえば、実装されている各種セキュリティ対策の大部分をすり抜けてしまうことになる。そもそも、インターネットに面してない各種システム環境は、脆弱性対策の優先度が低く、場合によっては未対策ですらあることも多い。VPN だけの話ではなく、クラウドサービスとのシステム連携等でアクセスを許可している内部環境も存在するかもしれない。もしそうであれば、極めて容易に不正アクセスを可能とする状況であり、攻撃者からの格好のターゲットとなり得る。つまり、安全な環境とそうでない環境が混在した状態になりつつあるということだ。

ゼロトラストによるセキュリティの確保

そこで登場するのがゼロトラストという考え方である。これは、2020 年に NIST（米国立情報技術研究所）発行のセキュリティ文書 SP800-207 において、その考え方や基本的なアーキテクチャが定義されている概念だ。

ゼロトラストでは、性悪説に基づき、次の 3 つの考え方により安全性を確保する。

・社内や内部だからといって安全な環境とは見なさない
・すべてのリソース（システム、サービス、情報等）へのアクセスを制御する
・ポリシーは状況に応じた信頼度により動的に見直し適用する

ここで気をつけていただきたいのは、ゼロトラストは、従来実施していた境界防御を完全に否定しているものではないということだ。今まで重要視していたインターネッ


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-207（Final）
「Zero Trust Architecture」（2020 年 8 月 11 日）
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf