SQAT® Security Report

2022年 春夏号

堅牢なセキュリティを考える

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

便利で安全なネットワーク社会を創造する
株式会社ブロードバンドセキュリティ

ごあいさつ

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

2021年は、ランサムウェアを中心にサイバー攻撃が激化の一途を辿りました。攻撃者の手口はより巧妙になり、Log4Shellのような重大な脆弱性情報が周知されれば、直後にはそれを利用した攻撃が発生したという報道もありました。JNSAが毎年発表している「セキュリティ十大ニュース」においては、例年半数ほどランクインしていた法制度関連のニュースがすべてランク外となり、その代わりに攻撃関連のニュースで埋め尽くされました。法執行機関やセキュリティ関係者の努力もあって攻撃者の逮捕も報道されるようになりましたが、攻撃者は増え続けており、2022年も事態は予断を許さない状況であるといえるでしょう。

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2021年下半期（7月～12月）の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。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。

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。**

SQAT.jp

堅牢なセキュリティを考える

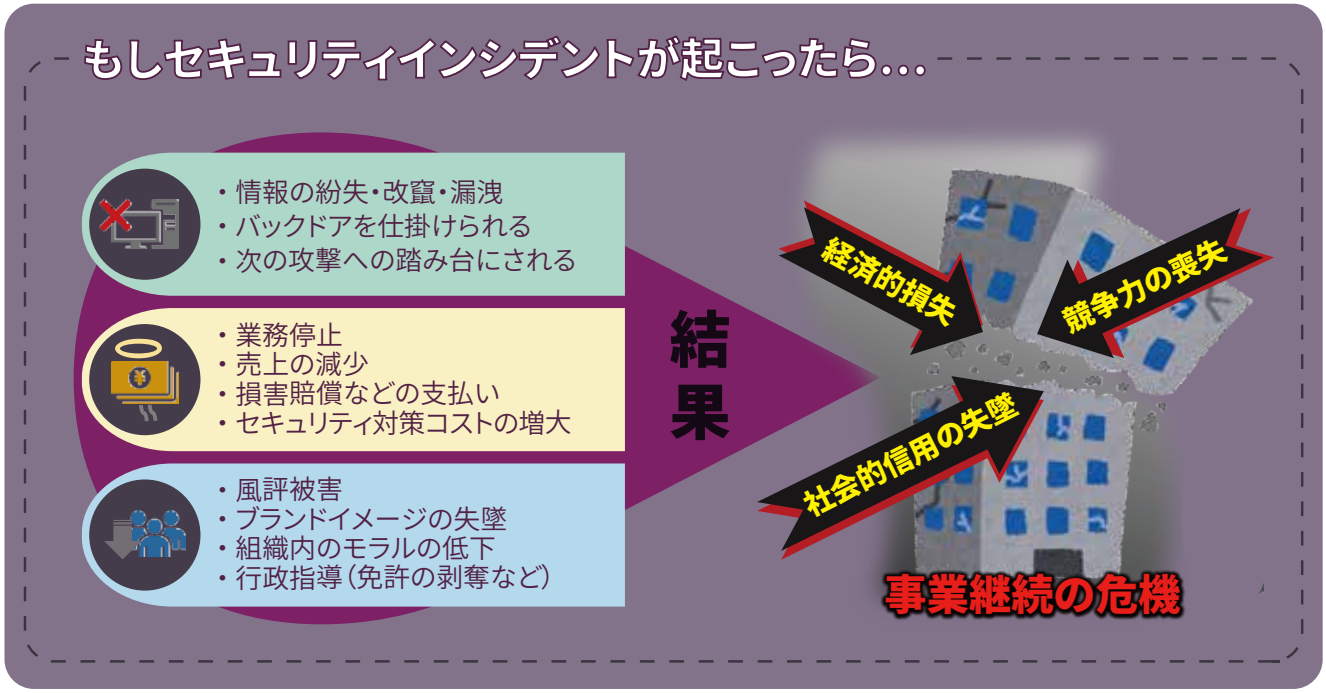
国内外問わずサイバー攻撃やセキュリティ対策に関する報道が飛び交っている。報道をさらりと読むだけでわかることは少ない。最新情報を抑えたくても追い切れないのが現実である。本稿では、当社アナリストの見解も交えてセキュリティ脅威や対策などを考察。堅牢なセキュリティについて探る。

SQAT® Security Report 編集部

なぜセキュリティ対策は必要なのか

セキュリティは日々状況が変わっていくため、リアルタイムでの情報収集が必須だが、そのためにセキュリティ動向を常に追いかけるのは一苦労である。労力や時間を掛けても、セキュリティにおいては「何も起こらないこと」が成功であるがゆえに、何かを得られている感覚があまりないと感じる企業や組織も少なくはないだろう。それでもセキュリティ対策は行うべきである。その理由を図1にまとめた。

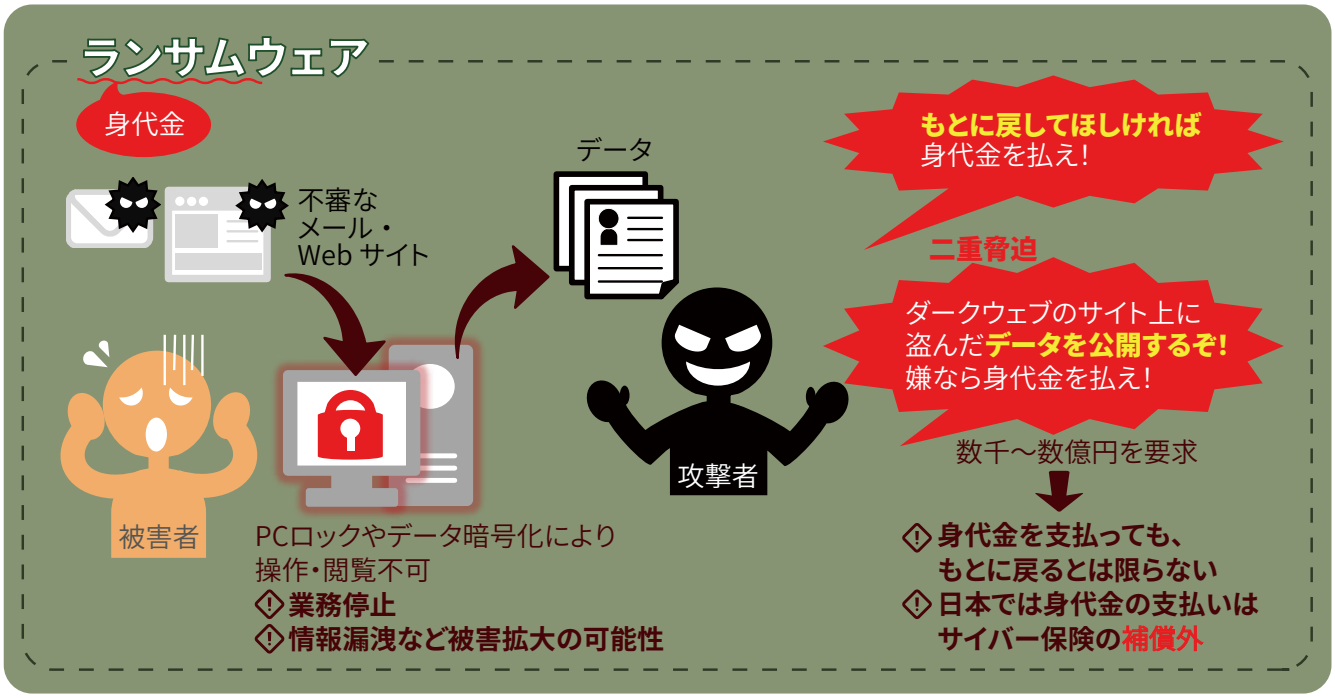
図 1



サイバー攻撃の紹介

企業の事業継続を揺るがすセキュリティの脅威。その被害を受けないためにも、セキュリティ対策は企業にとって欠かすことのできないもの。対策の対象となるサイバー攻撃は多数存在しているが、その中でも近年のセキュリティを語るうえで避けては通れない「ランサムウェア」について図2で紹介する。

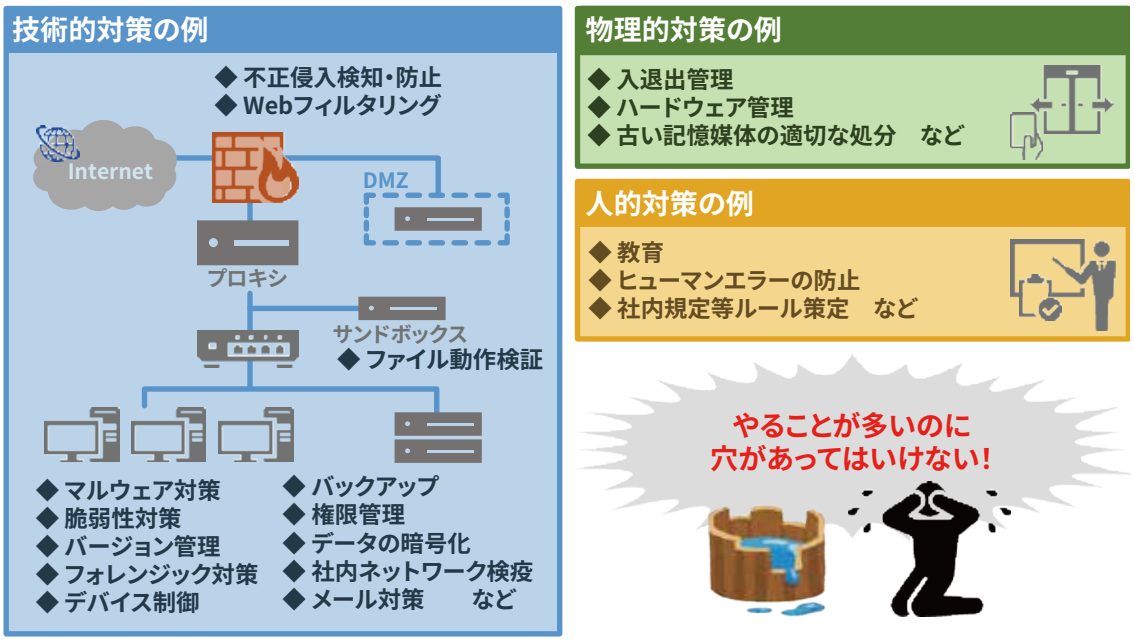
図 2



セキュリティ対策の例

「情報は第四の経営資源」と呼ばれるほど情報資産の価値が上がっている昨今において、あらゆるサイバー攻撃から情報資産を守るためにも、セキュリティの対策は必要不可欠である。しかし、セキュリティ対策と一言でいっても、多様な対策が内包されており、網羅的に対策を行うのは至難の業。それにも関わらず、どこか一つでも穴があるとリスクが高まってしまう。図3に対策の例を挙げた。

図 3



一組織でセキュリティを網羅する難しさ

ここまで見てきたようにセキュリティ対策は非常に重要なものだが、それを網羅的に過不足なく行うには膨大な労力と時間が掛かる。自組織にあったセキュリティ対策を効率よく行うには、セキュリティに関する膨大でタイムリーな知識と、セキュリティに専念できる時間、そしてそれらを行うことのできる人材が必要だ。しかし、セキュリティ人材の不足がこれまで啓蒙され続けていたとおり、それを一組織内で補うことが厳しいケースもあるだろう。また、たとえ網羅的に対策を行ったつもりでも、脆弱性診断など第三者の目によって診断を行うと、一つの目線では見えなかった弱点が見つかることもある。

一組織として網羅的に、そして最新の動向にあったセキュリティ対策を行うことは難しい。だからこそセキュリティの専門家による脆弱性診断など、自組織の状況にあった専門的サービスを活用するべきである。自組織の状況にあわせて賢く専門家を頼るのが、効率的な対策への大きな一歩となるだろう。

図 4