講演レポート

クラウドセキュリティによる危機管理と企業経営リスク

神戸大学大学院　工学研究科
教授　森井 昌克　氏

■ランサムウェア対策について

昨今、「セキュリティを重視すべきである」をテーマに雑誌への寄稿や講演などを行っているが、その中でクラウドと物理的につながっているストレージの世界でセキュリティを重視すべきか、について関連した記事を公開している。

昨年公開された記事には、ランサムウェア、クラウド、オンプレ会議、ハイブリッドクラウド、マルチクラウドといったキーワードが挙げられてよく議論されているが、特に不正アクセス事件等により、ストレージに注目が集まった年であった。

セキュリティ企業の株式会社ラックが公開したサイバー救急センターレポートではランサムウェア、bot、マルウェア関連が問題視されている。

ランサムウェア対策として、2020 年 1 月にセキュリティ企業 ESET 社との共同研究で復旧対策ツールを開発した。セキュリティ対策全般の流れとしては、これまでの「予防重視　→　不正アクセスからの防御」から、たとえ被害にあってもゼロになるような対策を行う、いわゆる 「リスク管理」を重視する流れに変わってきている。すでに、感染しても USB で復旧できるシステムを開発済みではあるが、まだ公開はしていない。このシステムは大概のランサムウェアに対し、自動復旧可能となっており、日々対策について考えているところである。

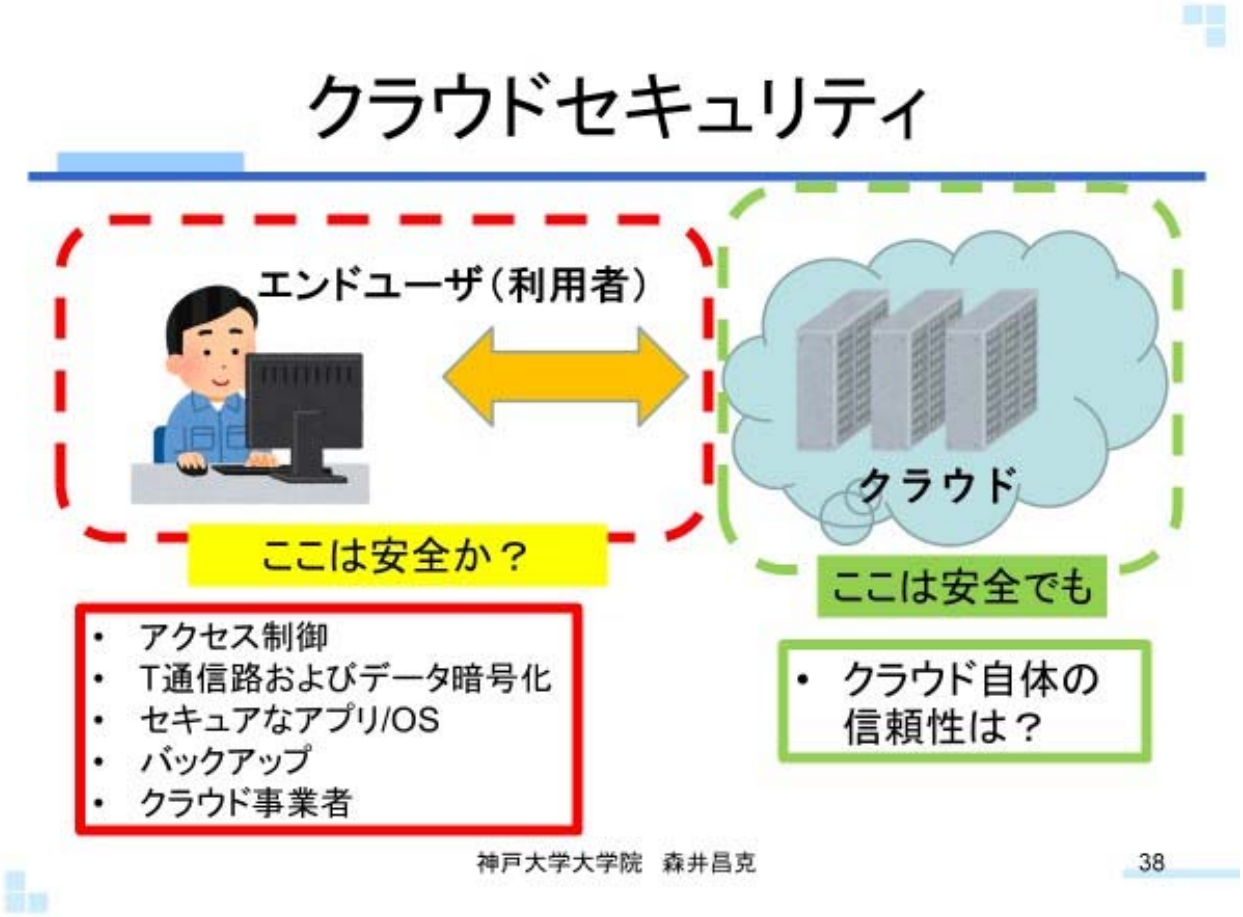
■中小企業でマルウェア感染の被害拡大

大企業の場合は被害をニュースなどで把握できるが、では、中小企業についてはどうなのか？ここ 1 ～2 年、残念ながら対策を講じていつつも、多くのマルウェア感染被害を受けているのが現状で、ようやく中小企業が狙われていることが知られるようになってきたところである。ほとんどの中小企業が被害を受けつつも、実際には気づいていないことが、ある実験を通して確かめることができた。

ある実験で、大学機関が持つダークネットといわれる未使用の IP アドレス 16,000 個を 24 時間監視し、不正や故意、マルウェア感染による不正アクセスを確認した。また、今年 1 月には、関西の中小企業 14 社が、故意にマルウェアを仕込もうとする不正なパケットをダークネットに送っていたことがわかった。たとえば感染被害に遭っているというセキュリティメッセージの警告を放置したまま、結果として他社まで感染させてしまう、という状況に気づいていない企業が多く、よう

やく中小企業が被害を受けていることが認知されるようになり、政府機関等が最新 OS のパッチ、対策ソフト導入など、“当たり前の”セキュリティ対策の実施を推奨しているがなかなか対策は講じられていない。中小企業の経営層や社員のセキュリティ認識が低いことや、サイバー社会に対する倫理モラルが浸透していないために、感染被害や情報流出を免れないのが現状である。

クラウド自体は安全であるとされているが、エンドユーザ側においては必ずしも安全とは言い切れない。エンドユーザがどう使うのか、暗号化、アクセス制御、セキュアな OS やアプリ利用などの問題点も多いが、クラウドの安全性を保障して、どう使うべきかが課題となる。



マルウェア自体がなくなることはないため、感染をどう防ぐか、が重要となる。中小企業のほとんどがアンチウイルスソフトを導入していながらもかなりの企業が被害を受けている現状から、マルウェア対策ソフトの導入だけでは感染を防ぐことは不可能である。IPA が発表した企業におけるセキュリティ 10 大脅威では、5 年以上「標的型攻撃」が 1 位を占めており、対策ができていないのが現状である。実際、企業を対象としたサイバー攻撃被害調査※1 の結果で、対策ソフトを導入していながらも、勝手にソフトを無効化するなどで、マルウェア侵入や情報流出などの企業にとって深刻な被害が検出されている。これまでに行ったサイバー攻撃被害調査では、マルウェア侵入、情報流出、ビジネスメール詐欺やネットバンクの不正送金、遠隔操作など、いずれも多くの被害結果がみられ、多くの中小企業が標的となり、被害総額も高額となり回収もできない状況になっている。

日本の中小企業や個人が標的となるケースが多くみられているのは、日本はセキュリティ意識が低いことが明らかになったのも要因の 1 つである。

違法取引サイト（ダークウェブ）は一般ユーザがみることが困難なサイトであるが、マルウェアや標的型攻撃メールによ

り、企業情報やメールのやり取り、決済のやり取り等を洗い出してビジネス詐欺メールや不正送金等に利用されている。

※1 「平成 30 年度中小企業に対するサイバー攻撃実情調査（報告）」
（共同研究実施者）大阪商工会議所、国立大学法人神戸大学、東京海上日動火災保険株式会社
http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/20190703cyber_h30.pdf

■サイバー攻撃被害の把握と早期発見・対策

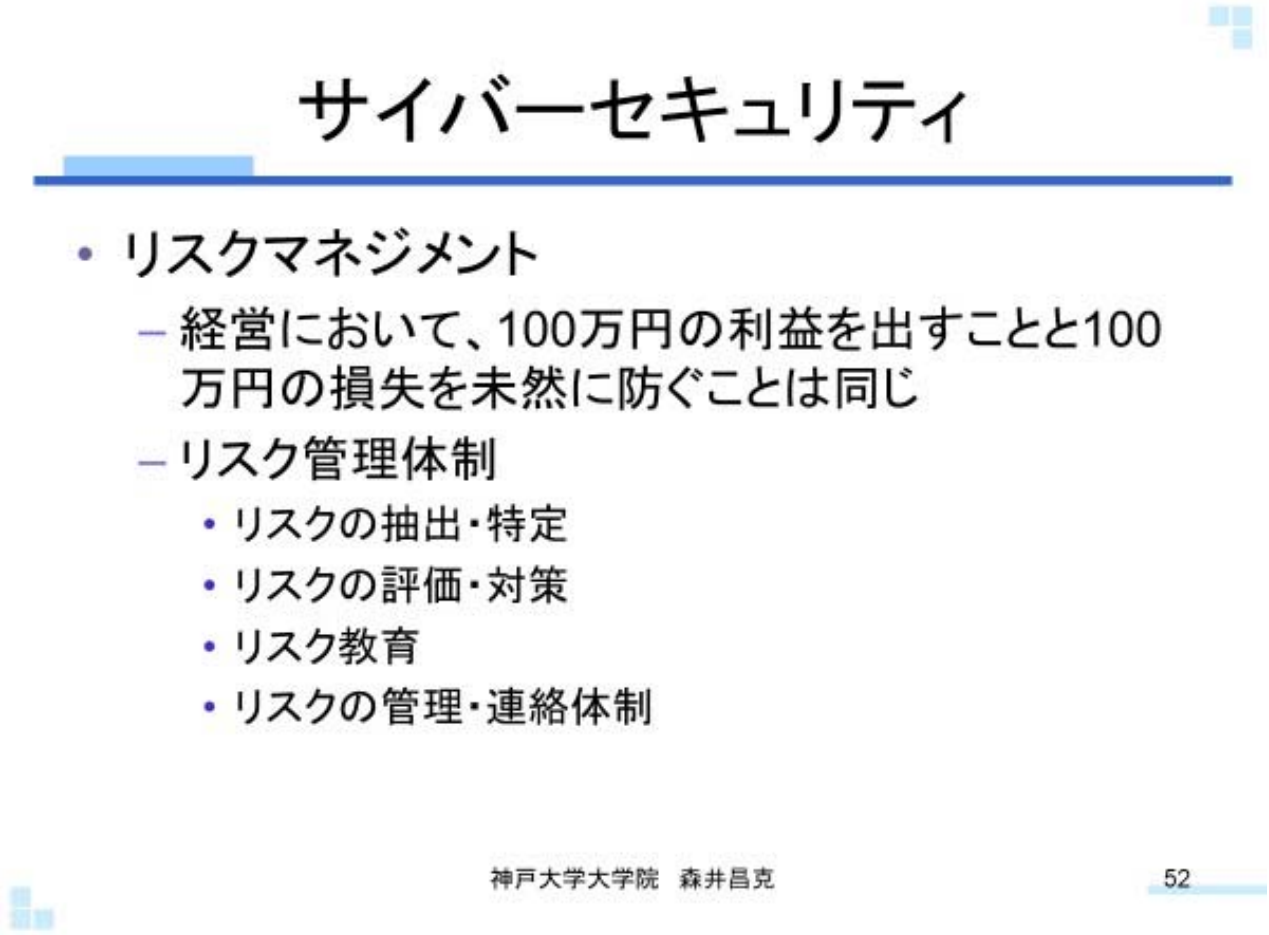
企業ではセキュリティ教育の一環として「標的型攻撃メール演習」が行われることが多いが、この演習の本来の目的は、うっかりあけてしまう者を減らすことだけでなく、メールをあけてしまった者が次にどう対処すればよいかを考える、つまり危機管理のための演習なのである。たとえ 1 人であっても標的型メールを開封してしまえば、マルウェア感染被害にあってしまうことから、リスクを最小限に抑えるために、メールを開いてしまった後にどう対処すべきか、を考えることが重要なのである。

サイバー攻撃の本質とは「攻撃をわからないようにすること」である。被害にあっていること自体が発覚できないのが現在のサイバー攻撃の特徴であるため、最近のサイバー攻撃の状況を把握し、どのような対策を講じるべきかを検討することが重要である。また、早期発見が困難であることを承知しておくことも必要である。被害を最小限に抑えるための早期発見、早期対策をどうするか、が考えられている。

■リスクマネジメントの重要性

物理社会においては、昔からリスクマネジメントが実施されている。大きな事故を起こさないようにするにはどうすべきか、というのは企業にとって重要であり、「安全」についての基準やガイドラインも以前からある。サイバー社会でも同様で、「安全」は企業にとっての価値であり、企業の競争力の要である。そのため、昨今のサイバーとフィジカルが一体化しつつある社会においても、安全とセキュリティを一体化して考える必要がある。

そこで大事なのは、セキュリティをどう捉えるかである。適切なセキュリティ対策をとらないと損失につながってしまうことから、リスク管理の実施が重要となる。リスク管理、つまりリスクマネジメントの手法は様々だが、その根本となるのは何がリスクか、どれだけのリスクが自社にあるか等を把握し、それらが自社にとってどれだけ大きなリスクになっているのかを計算して、セキュリティへの予算充当、人の配置をどうすべきか等の判断を行うことである。



セキュリティ対策はえてして裸の王様になりがちで、実施していると思っていても実はまだまだだったということが多い。そのため、セキュリティ対策をやっているから大丈夫！ではなく、リスクマネジメントによって自社のリスク（損害額）を評価し、セキュリティの実態を把握したうえでセキュリティ対策を考え直すことが重要なのである。