SE Report

サイバーセキュリティについて

株式会社コモドジャパン　執行役員 COO
営業推進部　部長

川口　賢 *Ken Kawaguchi*

1. はじめに

私達の生活に欠かすことのできないインターネットは、なくてはならない社会基盤として、その利用率がますます高まってきています。そうした中、日本企業に対するサイバー攻撃が急激に増加しています。

サイバーリスクに備えセキュリティ対策が急務とはいえ、その対策を行うためにシステムの改修やアップグレードなど、新たなリスクが発生するケースも珍しくありません。また、高い費用を掛けても100％の万全な対策が望めないことから、費用対効果が見えづらく予算の確保が難しいという声もよく耳にします。そのため攻撃のターゲットは、厳重に対策された大企業から、十分な施策を講ずることのできない中小企業にシフトしています。

サイバー攻撃に関する事前対策と事後対策について紹介します。

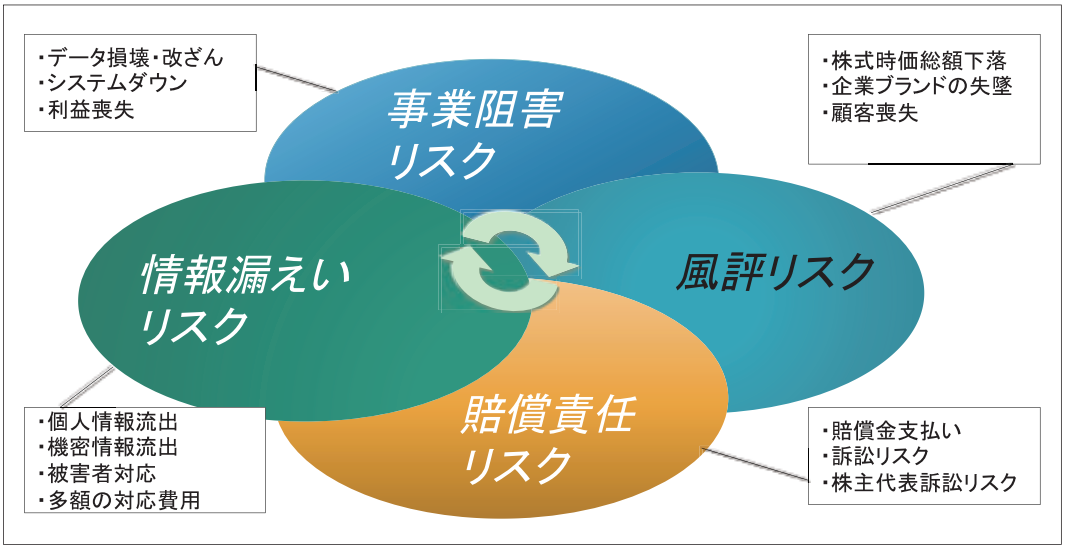
2. サイバー攻撃の脅威について

サイバー攻撃は、組織に対し様々な悪影響を連鎖的に及ぼす経済リスクであり、主に事業阻害リスク、情報漏えいリスク、賠償責任リスク、風評リスクの四要素があげられます（**図1**）。

その中でも、風評リスクについては株式時価総額下落、企業ブランドの失墜、顧客喪失などにより、重大な影響を与えるケースが少なくありません。リスクをあらかじめ試算しにくい面もあることから、情報漏えいなどにより企業の存続ができなくなるケースも少なくありません。

また、サーバを乗っ取られサイバー攻撃の中継地点（踏み台）として、ほかのサーバを攻撃するケースも数多く確認されており、こ

図１　サイバー攻撃が及ぼす経済リスク



の場合、乗っ取られたサーバを管理する組織は、サイバー攻撃を受けた被害者というだけでなく、一転して加害者という立場から損害賠償や刑事責任を負わなければいけないこともあるため、それらを想定した十分な事前対策を行うことが必要です。

3. サイバー攻撃のトレンドと増加状況

近年、サイバー攻撃に関わるインシデントは年々増加していますが、特に標的型サイバー攻撃となりすましメールが非常に増加しており、2016年の調査[1)]では、およそ10社に1社の割合で攻撃を受けています（**図2**）。

標的型サイバー攻撃とは、むやみやたらにウイルスメールを送りつけるのではなく、正当な業務や依頼であるかのように見せかける件名や本文でメールを送りつけ、受信者がだまされやすいような工夫がしてあります。

図２　標的型メール攻撃の件数推移

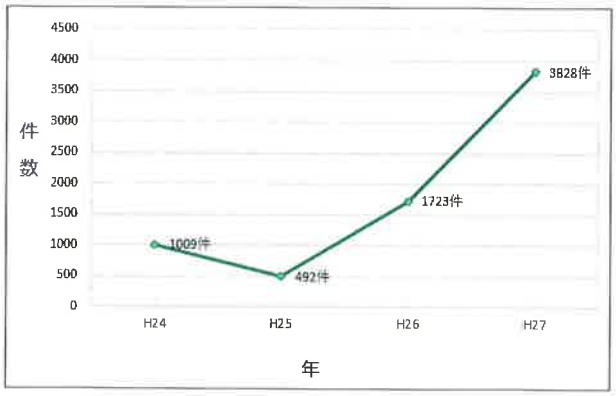
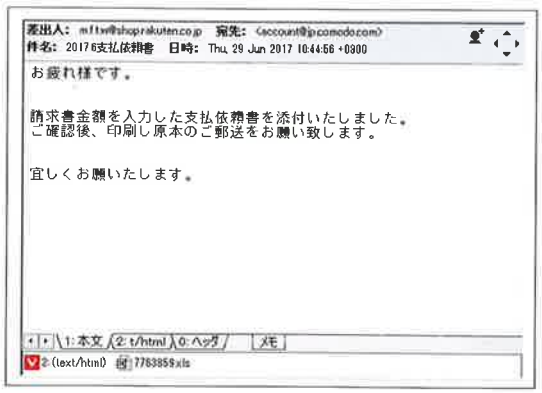


図３　標的型サイバー攻撃の一例



※1
ランサムウエア
感染したパソコンのファイルを暗号化することによって使用不能にした後、元に戻すことと引き換えに「身代金」を要求する不正プログラム。

従来は外国語のメールが多かったため、受信者の多くは直感的にゴミ箱に捨てていましたが、昨今、違和感のない日本語でのメールが増えたため、うっかり添付ファイルを展開するなどにより、不正なプログラムをインストールしてしまうケースが増加しています（**図3**）。

以前の攻撃者は自分の力を誇示するため、もしくは自己満足などの愉快犯が多く見受けられましたが、近年では明らかに金銭的価値を求め、個人情報や機密情報または直接的に金銭を要求するケースが多くなっており、攻撃者の組織化も進んでいます。

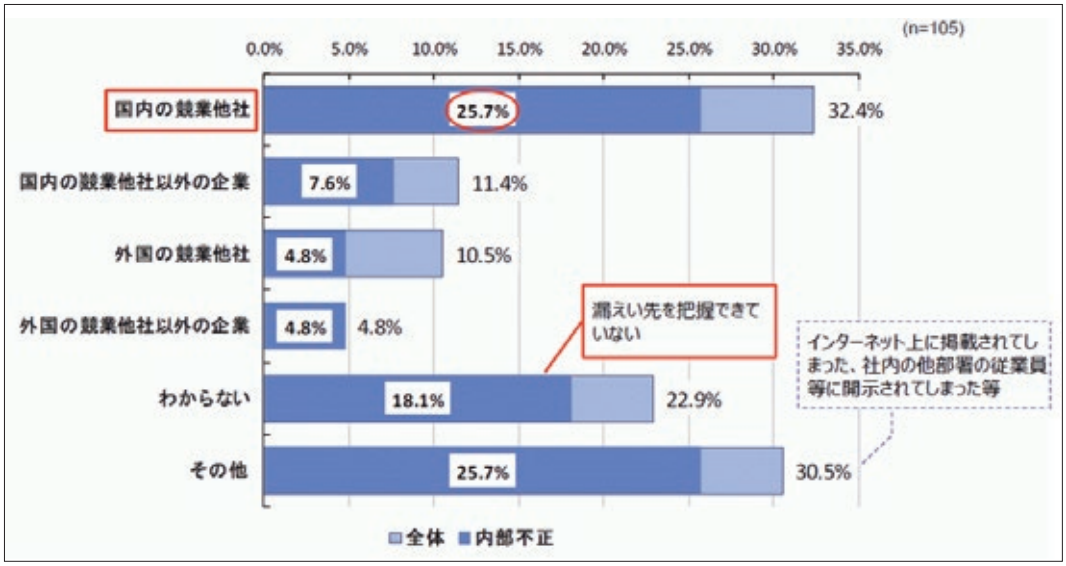
攻撃内容もDos攻撃などによるサーバへの侵入目的から、標的型メールやランサムウエア※1が主流となり攻撃手法がより複雑化しているため、以前は送信元や送信先のIPアドレス、ポート番号、またはプロトコル種別により、通信を許可したり遮断したりするなど、ネットワークを行き来するパケットを制御するパケットフィルタリングなどにより防御できましたが、現在はその通信が目的とするアプリケーションやコンテンツを確定した上で、正規なプログラムなのか不正なプログラムなのかを解析し、アプリケーション単位で細かな制御を行うなど、より複雑な防御方法が必要となってきました。

また、主流となる攻撃パターンに加え、従来の古い手法の攻撃も継続されるため、年々対策ツールの数が増え運用コストが膨れ上がるため、予算確保が難しい中小企業では、常に最新のツールを導入することが難しい状態が続いています。

4. 内部犯行について

サイバー攻撃というとインターネット経由でと思いがちですが、ソーシャルハッキングという手法が古くから存在します。この手法

図４　情報漏えい先の実態



は特別な知識や技術は不要で、その組織の社員や契約社員、関係者などがパスワードを本人から直接聞いたり、キーボードにパスワードを打ち込むのを後ろから盗み見たり、パスワードが書かれたメモをゴミ箱から入手するなど、あの手この手でパスワードを入手し、社内ネットワークに侵入することで個人情報や機密情報を盗み出し、競合他社や関連企業に転売する犯行が多く見受けられます(**図4**)[2]。

組織内関係者が犯行に関わる場合、その被害や情報は外部に公開されないケースが多く、また報道もされないことから、あまりご存知でない方もいらっしゃいますが、近年、非常に多くなっています（**表1**)。

米国のインターネットセキュリティ対策機関（CERT：Computer Emergency Readiness Team）によると、外部または内部犯行によるインシデント発生時について、どちらの被害額が大きいかの質問に対し、外部からの攻撃が38％、内部犯行が33％であるとの回答から、組織が受ける被害額の大きさでは同程度の割合となっており、外部と同様、内部対策についても有効な対策を講じる必要があります。

表１　主な内部不正事件の例

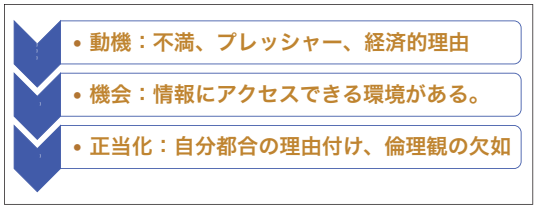
報道月	事件の概要	動機
2017年2月	J社の社員が製品の技術情報を漏洩し逮捕	製品を製造販売しようとした
2017年2月	オンラインショップのプラットフォーム提供会社の社員がネットショップ運営者情報を含む32,800件の個人情報、営業関連データを社外に持ち出し	不明
2016年6月	プロパン会社の社員が顧客情報等を不正に取得し同業他社に開示し逮捕	所属企業への不満
2016年2月	執行役員が子会社に出向中、主力製品の情報を転職先企業に開示し逮捕	利益取得
2015年9月	市職員が約68万件の有権者情報を自宅に持ち帰り、外部に流出させ懲戒免職処分	システム開発販売
2014年7月	顧客 DB を管理するグループ会社の業務委託先社員が個人情報を流出させ逮捕	金銭取得

5. 内部対策（トリガー対策）

独立行政法人情報処理推進機構によるアンケートの結果、その犯行動機は「会社や上司への不満・恨み」、「待遇の不満」、「プレッシャー」から発生するケースが多く、一個人が情報にアクセスできる環境が身近にあり、犯行に及ぶにあたり、自分に都合の良い理由付けまたは正当化ができる場合に発生します。

インターネット向けの対策は様々あり、専門のベンダーに依頼しコストをかけることでセキュリティレベルを向上させることができますが、内部犯行については、トリガーとな

図５　内部犯行のトリガー



る要素を一つ一つ排除する努力を行うことが組織として重要です（**図5**）。

それは、職場のストレスを低減する対策や職場環境の改善、社員それぞれのコミュニケーション向上、モチベーションアップの推進があげられ、その効果は生産性にもプラスとして作用する最良の施策であると考えます。

6. 内部対策（アクセス管理）

社内ネットワークには機密情報が保存されています。その情報は、経営層、経理や研究開発など、それぞれの部署以外の社員が閲覧できてしまう状態や上書きまたは削除されることがあってはなりません。

社内ネットワークのセキュリティを担保するには、適切なアクセス管理・機密情報へのアクセス制限、アクセスログの記録、定期的な監査・監視が必要です。

また、犯罪を予防するためには、アクセスログを監視（記録）していることを社員に周知させることも有効です。

これらの対策は、情報を取り扱う部署の業務内容および職務の変化や、人員の増減などにより、アクセス制限にセキュリティホールが生じてくるケースが見受けられるので、定期的な診断と改善が必須となります。また、外部からの攻撃に備え、インターネットから完全に分離したイントラネットを構築することは最も重要です。仮にデータが盗まれたとしても犯罪者がそのままでは利用できない形に暗号化し、データを分散して保存するなどの対策を行うことで被害を最小限に抑えることが可能です。

7. 内部施策（セキュリティ教育）

セキュリティ対策に高いコストをかけても、たった一人の行為でセキュリティインシデントが発生します。

ウイルスメールによる感染、USB メモリなどによるマルウエア感染、不正サイト閲覧による感染など、個人の操作や行為をトリガーとするインシデント予防には、社員一人一人のセキュリティ意識の底上げが必要で、システムを安全に利用し情報漏えいを防ぐことを目的としたセキュリティ教育が重要です。

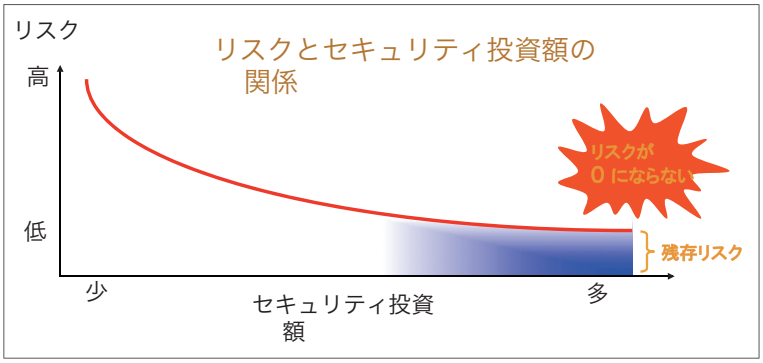
データに関する取り扱いルールの策定、周知、実行、定期的な評価と見直し、再教育を行い継続的な改善が必要であり、トレンドとなるサイバー攻撃に関する基礎知識を含めるためにも定期的な勉強会が有効です。また、リテラシーの高いと思われる管理職に対しては「慣れ」や「習慣」によるセキュリティリスクの理解を深めることも重要な要素です。

8. 事後対策

サイバーリスクに備えセキュリティ対策を行うためにシステムの改修やアップグレードを行うには、ソフトウエアの相性や周辺機器の挙動など、新たなリスクが発生するケースも珍しくありません。そして、高い費用をかけても100％の万全な対策は望めず、残存リスクがゼロになることはありません。

残存リスクが存在する以上、組織として何らかの対策を講ずる必要性があり、突発的な予期しない出来事が発生した際、資金的なインパクトを最小限に抑えるための対策が重要

図6　リスクとセキュリティ投資額の関係



です（**図6**）。

リスクの顕在化による予想以上の損失は、財務基盤の劣化を招き事業継続計画（BCP）や企業存続に大きな問題となるため、それらリスクを社外に移転するツールとして有効なのが保険の活用です。保険の活用は「残存リスクに対応することができる」ことと「実損害額の見える化」の2点が最も大きなメリットです。

前述のソーシャルハッキングや、ソフトウエアのセキュリティホールが公開され、その修正プログラムが提供される前にアタックするゼロデイ攻撃など、事前に十分な対策ができない残存リスクや、予算やソフトウエアの相性などで物理的にシステムを改修できない場合にも有効です。

また、実損害額の見える化については、事故が発生した際、様々な費用負担が大きくのしかかってきますが、それら直接的な対応費用は保険で対応できるため実際に支払わなければならない金額があらかじめ想定することができ、対策しやすいというのが組織にとって大きなメリットとなります。

企業を守る保険にはいろいろな商品があり、すでに何らかの保険に加入されている組織がほとんどかと思いますが、そこにも落とし穴があります。実際に事故が発生し保険会社に相談したら、保険が下りなかったというケースも多々あります。「保険の内容を正確に把握せず契約してしまった」、「必要な補償がオプション扱いだった」などを耳にしますので、保険の加入や見直しの際は、信頼のおける保険会社と営業担当者の選別が重要です。

9. 最後に

セキュリティ対策に完璧はありません。そして、完璧を目指すほどに費用対効果が悪くなります。

少ない予算、限られたリソースの中で対策を行うには、絶対に失えない資産、失っても再構築できる資産など、資産の優先付けを再確認した上で事前対策を行い、残存するリスクを自社で担保できるのか、または保険を活用するのか、トータルで計画するのが最善の方法です。

参考文献

1）警察庁：平成27年・平成28年におけるサイバー空間をめぐる脅威の情勢について，2016.
2）（独）情報処理推進機構：企業における営業秘密管理に関する実態調査報告書，2017.

かわぐち●けん

2002年インターネットサーバサービスを基盤事業とするプロックスシステムデザイン（株）に入社。2008年同社とインターネットセキュリティにおけるリーディングブランドCOMODOが出資する（株）コモドジャパン設立後、しばらく2社の業務を兼務するが、現在は専任で世界規模でのセキュリティ向上に積極的な支援と活動を行っている。