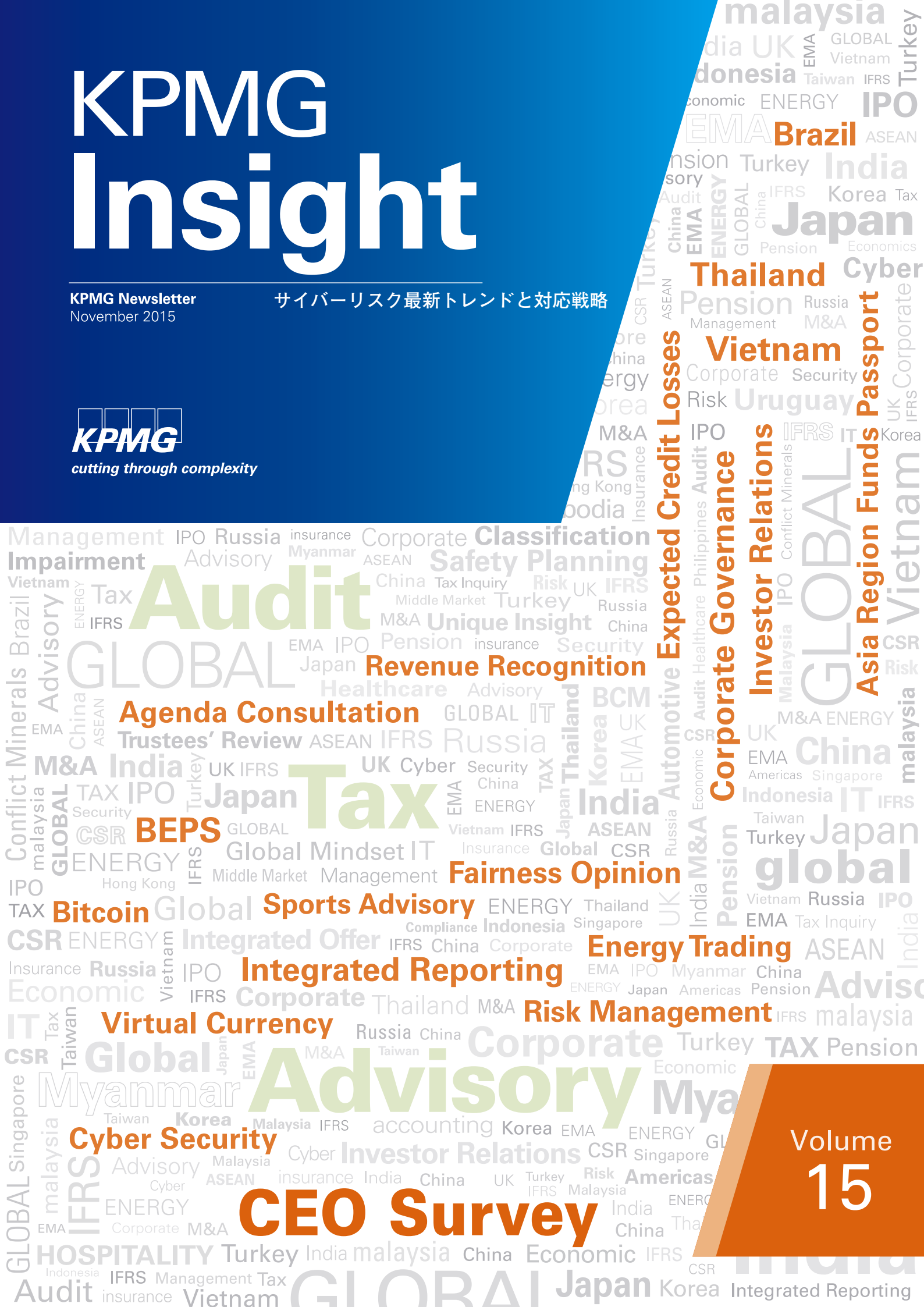
KPMG Insight

KPMG Newsletter
November 2015

サイバーリスク最新トレンドと対応戦略

KPMG
cutting through complexity



サイバーリスク最新トレンドと対応戦略

KPMG コンサルティング株式会社
サイバーセキュリティアドバイザリー
ディレクター　小川　真毅

小川（おがわ）　真毅（まさき）
KPMG コンサルティング株式会社
サイバーセキュリティアドバイザリー
ディレクター

サイバーセキュリティ基本法、マイナンバー、東京オリンピックなど、国家レベルで様々な環境変化が巻き起こり、IoT、ビッグデータといったテクノロジー環境も急速に変化するとともに新たなビジネスチャンスが次々と創出される中、巧妙化・大規模化するサイバー攻撃による情報漏えいや被害の発生は後を絶たず、ステークホルダーへの説明責任を含めてサイバーリスクへの対応は経営課題として取り組むべき状況となっています。

サイバー脅威の変遷に伴って組織がサイバーリスク対応能力を強化するためには、“既知”の脅威を前提にした従来型アプローチから脱却し、「インテリジェンス」と「レジリエンシー」機能を高めて“未知”の脅威に立ち向かう新たな戦略が必要です。

そこで、本稿では、国家的事案となっているサイバー攻撃の現状を紹介するとともに、テクノロジー環境の進化に伴うサイバーリスク、サイバー脅威の変遷、そして、これからのサイバーリスク対応戦略について解説します。

なお、本文中の意見に関する部分は、筆者の私見であることをあらかじめお断りいたします。

【ポイント】

- 政府機関や重要インフラ事業者を狙ったサイバー攻撃は急激に増加しており、政府はサイバーセキュリティ基本法やサイバーセキュリティ戦略を通じて、国家レベルの事案としてサイバーリスク対応に取り組んでいる。
- IoT、制御システムのオープン化、ビッグデータ、アナリティクス、ソーシャルネットワークといったテクノロジー環境の変化は、ビジネス機会を創出する一方で新たなサイバー脅威も生み出し、実際に多くのインシデントが発生している。
- 組織がサイバーリスク対応能力を高めるためには、サイバー脅威を可視化し、知見を集積して対策に活かす「インテリジェンス」とインシデントから早期に立ち直る「レジリエンシー」を備えるとともに、経営層がイニシアチブをとり、KPI を設定してマネジメントしていく必要がある。

Ⅰ 国家的事案としてのサイバー脅威

『今朝、正式に閣議決定されました！』。2015年9月4日、筆者が衆議院議員会館で催されている“サイバーセキュリティシンポジウム2015”にて、午後最初の講演に耳を傾けようとした矢先、内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）代表者の第一声が勢いよく飛び出しました。

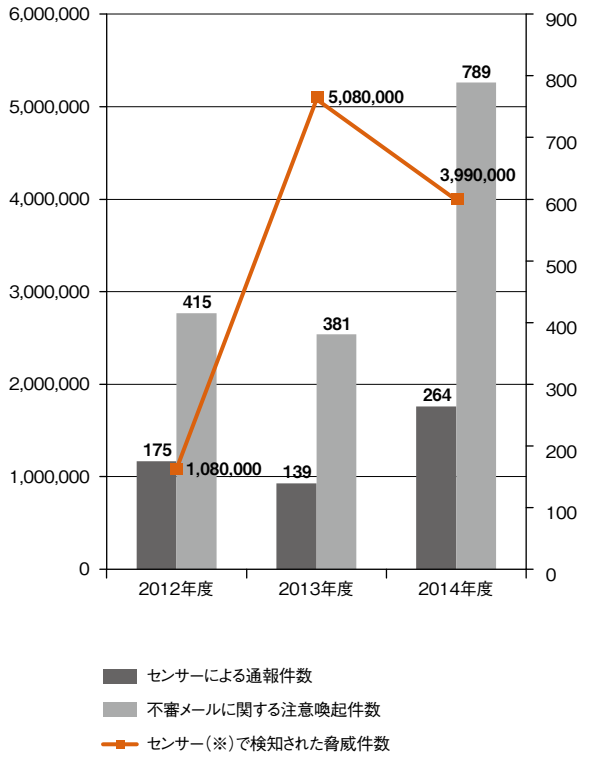
日本政府は同日午前の閣議で「サイバーセキュリティ戦略」を正式決定し、自由、公正かつ安全なサイバー空間を創出、発展させることを以って、経済社会の向上と持続的発展、国民の安全・安心な暮らしの実現、国際社会の平和・安定と安全保障に寄与する、としています。

これに先立ち、2015年1月9日には「サイバーセキュリティ基本法」が全面施行となり、国および地方公共団体のサイバーセキュリティ分野における責務を明確にし、「内閣官房情報セキュリティ対策推進室」を「内閣サイバーセキュリティセンター」に改組するとともに、その役割の明確化と権限の強化を行いました。

この背景には、2011年に発覚した政府機関や防衛産業系民間企業への標的型攻撃を皮切りに、2012年から2013年にかけて重要インフラ事業者に対するサイバー攻撃が倍増し、2013年から2014年には政府機関への不審メール件数が倍増するなど、政府機関や重要インフラ事業者を狙ったサイバー攻撃が本格化してきていると考えられ、もはや看過できない事態となっています（**図表1、2**参照）。

また、周知のとおり2020年には一大国際イベントである東京オリンピックの開催が予定されており、その成功には国家の威信がかかっていると言っても過言ではありませんが、前回大会であるロンドンオリンピックで電力供給システムや大会公式ウェブサイトを狙った大規模なサイバー攻撃が発生したことを踏まえ、東京オリンピック大会組織委員会は警備局内にサイバー攻撃対処部ならびにCSIRT（Computer Security Incident Response Team）を設置し、NISCや東京都と連携してサイバーセキュリティ対策にあたる体制を構築するとしており、サイバーリスクは国家の繁栄とサステナビリティを妨げる重要課題として対処すべき事案になっていると言えます。

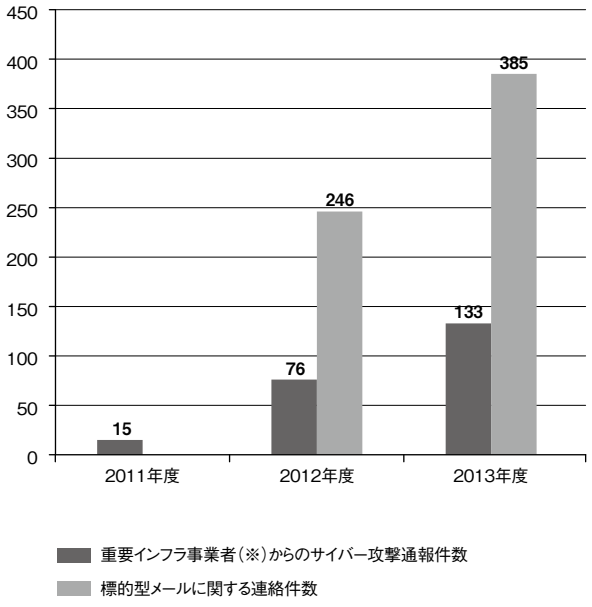
図表1　政府機関を狙ったサイバー脅威件数の推移



※センサーとは、GSOC（政府機関情報セキュリティ横断監視・即応調整チーム）によって各府省庁などに置かれたサイバー脅威検知システムを指します。

出典：内閣サイバーセキュリティセンター資料「サイバーセキュリティ政策に係る年次報告（2013年度）」（情報セキュリティ政策会議）をもとにKPMGが作成

図表2　重要インフラを狙ったサイバー脅威件数の推移



※重要インフラ事業者とは、「重要インフラの情報セキュリティ対策に係る第3次行動計画」（2014年5月19日情報セキュリティ政策会議決定）に基づき、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油の13分野を指します。

出典：内閣サイバーセキュリティセンター資料「サイバーセキュリティ政策に係る年次報告（2013年度）」（情報セキュリティ政策会議）をもとにKPMGが作成

Ⅱ テクノロジーとサイバーリスク

1. モノのインターネット

サイバーリスクは国家的事案であるとともに、民間企業や消費者にとっても身近で深刻な課題になってきています。昨今では「IoT（Internet of Things、モノのインターネット）」と呼ばれるとおり、あらゆる機器や装置がネットワークに繋がって情報をやり取りするようになっていくことから、これを多くの企業がビジネスチャンスと捉えて取り組み、消費者もより便利になる社会への期待に胸を膨らませていますが、テクノロジーの進化とサイバーリスクは表裏一体の関係にあります。

たとえば、自動車には様々な高精度センサーが搭載されて、状況に応じてアクセルやブレーキ、ステアリングが高度に制御されることにより、安全で環境にも優しいスマートドライブが可能となる一方、こうした電子的制御機能が無線などを通じてハッキングされることにより、不正に操作されたり制御不能に陥ったりするリスクが生じます。実際に2015年8月に米国ラスベガスで開催された世界最大級のサイバーセキュリティカンファレンスである“Black Hat USA 2015”にて、有名ハッカーがある大手自動車メーカーの人気車種のワイヤレス接続用パスワードを解読し、電子制御システムOS（オペレーティングシステム）の脆弱性を突いて侵入することで、カーステレオやワイパー、ウインカーに至るまですべてのコントロールを手中に収める様子を公開し、大きな注目を集めました。

家庭に目を移すと、猛暑日に外出先から帰宅する前に電車の中からスマートフォンを通じてエアコンを操作して冷房を入れておく、冷蔵庫の中身をデータ化しスーパーでの買い物中に確認することで買い忘れや買い過ぎを防ぐなど生活が便利になる一方で、こうした家電製品を遠隔から不正操作し異常な動作を引き起こして発火させる、防犯カメラの映像を外部から見られたり、カメラの機能を停止されてしまうなど、日常生活においてもサイバー攻撃の脅威にさらされる可能性が高まります。

その他にも、鉄道や航空などの交通インフラの制御システムが不正アクセスされて交通マヒや重大事故が発生したり、電力、水道、ガスなどの生活インフラがサイバー攻撃を受けて供給不能に陥ったりするなど、様々なリスクが懸念されていることも事実です。

2. ビッグデータ

テクノロジー分野においてIoTと比肩するように活発な取組みが行われているのが、「ビッグデータ」の領域です。2015年9月3日に可決、成立した「個人情報保護法」の改正案では、個人を特定できないように加工した情報を「匿名加工情報」と定義し、このように加工された情報であれば元の個人情報を提供した本人の同意を得ることなく第三者に提供できるという枠組みが規定されました。これにより兼ねてから情報の宝庫でありながらも厳しい利用制限が加えられてきた個人情報を加工したうえで積極的に活用していくことが可能となり、個人ごとの細かい購買行動を記録、分析して需要を予測したり、そうした膨大なデータの分析作業そのものをサービスとしたりするなど、新たなビジネスの創出に繋がることが予測されます。

さらに、2015年10月より番号通知が始まる「マイナンバー法」（行政手続における特定の個人を識別するための番号の利用等に関する法律）についても、当初予定されている社会保障、税務、災害対策の3分野での限定的な利用から、将来的には金融機関や民間サービスなどへの利用拡大も検討されており、マイナンバーと本人確認さえできれば、面倒な手続きを経ることなく速やかに様々なサービスが享受できる社会の実現に向けて動き出しています。

もちろんビッグデータとして取り扱われる情報は個人情報だけでなく、販売管理システムや工場の生産管理システムから得られる実績データや統計情報、IoTを通じてあらゆるモノから発信され、蓄積されていくデータなどもまた、その分析によって新たな価値とビジネスチャンスを生み出すタネとなります。

しかしながら、こうした価値のあるデータの集まりは悪用を目論む犯罪組織やハッカー集団からの格好の標的でもあり、記憶に新しい2015年5月には、某行政機関から101万件もの個人情報が標的型攻撃を通じて漏えいする事件が発生しています。そのため、今後ビッグデータやその分析（アナリティクス）によって競争優位性の獲得を目指す組織にとっても、サイバーリスクは切っても切り離せない課題であり続けると考えられます。

Ⅲ サイバー脅威の変遷

1. 攻撃主体や目的・手法の変化

国家や社会、企業活動や日常生活におけるテクノロジーへの依存度が日に日に高まっている状況に呼応するように、サイバー脅威もまたテクノロジーを駆使することでその巧妙さと熾烈さを増しています。

ほとんどの企業はインターネット上にウェブサイトを立ち上げ、自社の事業紹介やIR情報の公開、会員向けサービスなどを提供しています。拠点間だけでなくビジネスパートナーやサプライヤー、保守ベンダーなどの外部組織ともネットワークで繋がり、以前は情報システムから隔離されていた工場の生産システムや、電気・水道・ガスなどの社会インフラおよび航空・鉄道・道路などの交通インフラの制御システムにも、IoT

と相まってオープン化の流れが広がってきています。日常生活においては、電子決済やインターネットバンキングも普及が進み、ECサイト経由で日用品や食品、衣類、書籍など何でも手に入る時代となり、ソーシャルネットワークサービス（SNS）やインターネット上のコミュニティで様々な情報を発信し、交換するようになりました。

一方で、こうした環境は様々な目的を達成しようとする攻撃者にとってもその活動の場を増やすこととなり、以前は一部の愉快犯による自己顕示やいたずら目的でのハッキングが主流であったサイバー攻撃も、いまではその様相が大きく変わりつつあります。攻撃者は個人や小人数のグループから組織的な集団へと拡大しており、自国の防衛や敵対国を攻撃するためのサイバー部隊を公式または秘密裏に設置する国家もあります。これは、サイバー攻撃にはそれだけの費用と労力を注ぎ込むだけの魅力や価値があることを裏付けており、実際にサイバー攻撃による被害は全世界で100兆円規模にのぼるという推測をする専門家もいます。

これに伴ってサイバー攻撃の対象は、いたずらによる不満解消や名声を得たいという自己顕示などの精神的欲求を満たすためなら相手は誰でもいいという無作為型から、組織立てて狙うべき相手や情報資産などを明確に定め、情報の搾取や攻撃対象に損害を与えるという経済的利益追求のために攻撃する標的型へと変貌を遂げています。同様に、サイバー攻撃の手法においても、アンダーグラウンドなコミュニティなどで誰でも入手可能なウイルスやハッキングツールをそのまま利用するコモディティ型から、攻撃対象の環境や特徴に応じてやり口を変化させ、人の心理的脆弱性までも悪用するソーシャルエンジニアリングを含めた巧妙かつ複合的で予測困難なテイラーメイド型サイバー攻撃へと変遷してきています。

こうしたテイラーメイド型サイバー攻撃は、軍事行動における一連の行動になぞらえて2009年にロッキードマーチン社が「サイバーキルチェーン」という表現で提唱しており、攻撃者がいかに周到に準備し、手数をかけて標的を攻撃するかが分かります（**図表3**参照）。

2. 最新の主なサイバー脅威

昨今の巧妙化するサイバー攻撃手法について、その例をいくつか紹介します。

（1）インターネットバンキングを狙った不正送金

近年、インターネットバンキングのIDやパスワードなどが盗まれて口座から現金が不正送金される被害が多発しており、警視庁[1]の発表では2014年は1,876件で約29億円にのぼる被害が発生しています（2013年の被害額約14億円から倍増）。インターネットバンキングを狙ったサイバー攻撃は、IPA（独立行政法人情報処理推進機構）が有識者の投票に基づいて毎年選出、公表している情報セキュリティ10大脅威でも第1位に選

図表3　サイバーキルチェーン（テイラーメイド型サイバー攻撃）の流れ

1. 警察庁「平成26年中のインターネットバンキングに係る不正送金事犯の発生状況等について」（平成27年2月12日）
https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf

ばれており（昨年は第5位）、被害の拡大が懸念されています（**図表4**参照）。

図表4 情報セキュリティ10大脅威 2015

順位	タイトル
1	インターネットバンキングやクレジットカード情報の不正利用
2	内部不正による情報漏えい
3	標的型攻撃による諜報活動
4	ウェブサービスへの不正ログイン
5	ウェブサービスからの顧客情報の窃取
6	ハッカー集団によるサイバーテロ
7	ウェブサイトの改ざん
8	インターネット基盤技術を悪用した攻撃
9	脆弱性公表に伴う攻撃
10	悪意のあるスマートフォンアプリ

出典：「情報セキュリティ 10 大脅威 2015 ～被害に遭わないために実施すべき対策は？～」（独立行政法人情報処理推進機構　セキュリティセンター）をもとに KPMG が作成

インターネットバンキングを狙ったサイバー攻撃においては、最近では多くの場合実在する銀行やクレジットカード会社などを装って、パスワードの再設定依頼や支払い内容の確認などを求める電子メールをターゲットとなる一般の口座所有者や企業の経理担当者などに送信します。受信者が電子メール内にあるURLをクリックすると悪意のサイトに誘導され、口座番号やアカウント情報、パスワードを入力することで情報が搾取されたり、悪意のサイトから不正なマルウェアを自動的にダウンロードさせられて、次回以降実際にインターネットバンキングを利用する際に入力する情報をすべてアップロードするように仕組まれたりします。

この手法は従来使われてきたフィッシング詐欺をベースにしており、以前は電子メールの文面に違和感があったり、URLをクリックしてアクセスした先のウェブサイトが本物のウェブサイトとはレイアウトがかなり異なっていて気づいたりするなど、作りに粗さが目立ちましたが、最近の攻撃者は実際に銀行やクレジットカード会社が送信するメールをそのまま模倣し、ウェブサイトもまったく同じレイアウトと画像で作成されており、場合によってはあらかじめ攻撃対象者の情報をSNS上で収集し、興味を引きやすいように電子メールの内容を細工するなど、一見すると不正なものと見極めることが困難なほど精巧に作り込まれています。

(2) ランサムウェア

2014年後半から2015年前半にかけて、被害が急増しているサイバー脅威の1つに「ランサムウェア」によるものが挙げられます。アンチウイルスソフトウェア企業の調査[2]では、昨年まで国内では四半期に1件程度の被害報告しか確認されていませんでしたが、2015年第2四半期は17件へと急増しています。

ランサムウェアとは、実行すると端末上に保存されている様々なデータ（オフィスドキュメントや画像など）を勝手に暗号化してしまい、中身を閲覧できない状態にする不正ツールの一種で、当該データの復号化と引き換えに金銭を要求する文面が画面上に表示されます。この一連の事象が、人質をとって身代金を要求する誘拐犯の様であることから、「Ransom（ランサム：身代金）」と「Malware（マルウェア：悪意のプログラム）」を組み合わせてランサムウェアと呼ばれています。

特に最近被害が多発しているランサムウェアは当初よりも悪質化しており、この不正プログラムを実行した端末上のデータにとどまらず、共有設定されているファイルサーバ上のデータや、ネットワークドライブなども根こそぎ暗号化してしまうため、その影響は社内全体に波及し、甚大な被害をもたらす場合があります。なお、請求されたとおりに金銭を支払ったとしても復元してもらえる保証はなく、さらに高額の金銭を要求されるケースもあるため、絶対に要求にしたがってはいけません。

ある企業では、従業員が人事異動発令を装ったフィッシングメールに添付されていたファイルを不用意に開いてしまったことでランサムウェアに感染し、業務途上であった外部発表前のデータがすべて暗号化されて読み取れなくなり、データセンターの移行直後でまだバックアップシステムが稼働してなかったこともあり、止む無く復旧を諦めて一から再作成するという事態に陥りました。

(3) サイバーテロ

国際社会を含めてにわかに耳目を集めている脅威がサイバーテロリズムです。2015年6月に米国連邦政府の人事管理局がサイバー攻撃を受けて政府職員400万人分の個人情報が漏えいし、局長が辞任するまでに発展した事件がありました。米国政府筋によると、この事件には中国のサイバー攻撃組織が関与したとみられており、これ以外にも米国企業は中国側からのサイバー攻撃によって年間数千億円規模の経済的損失を被っているという試算もあるなど、国家間におけるサイバー攻撃はテロリズムの発露であるとも言えます。

隣国の韓国では、2014年12月に原子力発電所管理会社がサイバー攻撃を受けて内部文書が流出し、原子炉の設計図がインターネット上で公開されてしまうという事件も発生しています。原子力関連施設を狙った攻撃としては、2010年に発覚

2. トレンドマイクロ株式会社「Trend Labs 2015年第2四半期 セキュリティラウンドアップ」
http://www.trendmicro.co.jp/jp/security-intelligence/sr/sr-2015q2/index.html

したイランの核燃料施設を狙ったマルウェアである「Stuxnet（スタックスネット）」が非常に有名ですが、その後の注意喚起にもかかわらず類似の事件は世界各地で発生し続けており、2014年には欧州の電力会社を同時多発的に狙った「Havex（ハーベックス）」というマルウェアによって情報漏えいが引き起こされています。

こうした動向は日本にとっても対岸の火事ではなく、2015年3月には空港の公式ウェブサイトがサイバー攻撃によって改ざんされ、航空管制や離発着のシステムには影響がなかったものの、利用者や業界関係者をヒヤリとさせる事件になりました。

Ⅳ これからのサイバーリスク対応戦略

1. 経営課題としてのサイバーリスク

サイバー攻撃の巧妙化、大規模化に伴ってインシデント発生時のビジネスインパクトも増大の一途を辿っています。2013年11月に米国の小売企業に対するサイバー攻撃では、7,000万件の個人情報漏えいが発生し、対策費用は200億円以上となり、CEOの引責辞任にまで発展するという甚大な被害をもたらしました。また、2014年7月に国内の教育サービス企業で発生した2,070万件の個人情報漏えい事件では、顧客へのお詫びや再発防止施策など合わせて260億円にのぼる特別損失が大きく響いて上場以来初の赤字転落、担当役員であった副会長とCIOは引責辞任するという多大な影響を及ぼしました。

こうした事例に代表されるように、インシデントには組織のサステナビリティを脅かす様々な事態が付随しており、サイバーリスクは企業経営において対処すべき重要課題であることは明白です（**図表5参照**）。株主、顧客、規制当局、行政機関、社会といったステークホルダーは、経営者に対して積極的なサイバーリスクへの理解と対応を求める姿勢を一層強めています。

図表5 インシデントがもたらすビジネスインパクト

競争力低下／知財の盗難	ブランドイメージの毀損
法・規制違反に対する罰金	機会損失／時間的損失
保有資産の紛失	人的リソースの浪費

2. 従来型アプローチからの脱却

ウイルスや公開された脆弱性を悪用する攻撃などの“既知”の脅威がサイバー攻撃の多くを占めていた2000年代までとは異なり、2010年代に入る前後から活発化した標的型攻撃をはじめ、ターゲットに応じて巧妙に手口を算段するテイラーメイド型の攻撃は事前に予測することが困難な“未知”の脅威です。

インシデントが多発している現状を鑑みると、サイバー脅威の中心が“既知”から“未知”へと変遷するなかで、多くの企業は“既知”の脅威を前提にした以下のような従来型のサイバーリスク対応アプローチから抜け出せていないように見受けられます。

誤解① - 完璧なセキュリティを確立しなければならない

そもそもサイバーセキュリティをめぐる攻防においては、あらゆるセキュリティ上の欠陥（セキュリティホール）を塞がなければ完全に攻撃を防ぐことができない防御側に対し、1つでも穴があれば攻撃が成功する攻撃側が圧倒的に有利な立場にあります。まして有限の経営資源という制約がある企業にとって、予測困難な脅威が主流となっている現状で、すべてのサイバー攻撃を100％防ぎきることは世の中からすべての犯罪をなくすことに等しく、残念ながら現実的に不可能と言えます。

誤解② - 最新のテクノロジーを導入すればよい

サイバー攻撃対策はサイバー空間だけで完結するものではありません。確かに高精度な攻撃検知・防御テクノロジーを導入することで、多くの汎用的なサイバー攻撃を防ぐことができるようになりますが、標的型攻撃のように巧妙に関係者に成りすまして従業員に電子メールを送ったり、電話で取引先従業員を装って重要情報を聞き出そうとしたりするような人の弱みに付け込む行為に対してテクノロジーはほとんど無力です。

誤解③ - トップガンに任せておけば安心だ

サイバーセキュリティ分野において、極めて優秀なスキルと熟練した経験を持つエリートのことを、米国の映画になぞらえて「トップガン」と呼びます。インシデントの発生時には特にこうした人材の活躍により早期収束と復旧が期待できますが、社内でハイスキル人材を育成するには時間がかかるうえ、特定個人のスキルに依存したインシデント対応体制では、当該人物が休暇中であったり転職してしまったりすると途端に対応力が弱まることになります。

こうした従来型の誤ったアプローチを採ってしまう企業に共通することは、変遷するサイバー脅威の実態と、それらが組織に与える影響をタイムリーかつ適切に把握するための仕組みや取組みが欠けており、経営層がサイバーセキュリティ対策に関する正しい方針の提示と戦略の立案、および意思決定ができる環境にない、ということが考えられます。

ゆえに、まず従来型アプローチから脱却するためには、“既知”の脅威だけではなく、組織に固有の“未知”なるサイバー脅威を可視化するための仕組みを構築する必要があります。“未知”の脅威を可視化することなど不可能ではないかと思われるかもしれませんが、ここでいう可視化はある時点で見えているリスクを洗い出すという意味ではありません。そうした取組みも組織を取り巻くリスク環境を俯瞰的に把握するためにはもちろん必要ですが、日々刻々と変化し、進化するサイバー脅威に対し、今日存在していない脅威が明日も発生しないという保証はどこにもありません。いま必要なサイバー脅威の可視化とは、定期的な脅威の洗い出しとリスク評価に加えて、起こりうるシナリオを想定し先行して対策を講じるための判断材料を得ることを目的とした定常的な情報収集と分析、および監視・モニタリング活動を通じてサイバー脅威や攻撃兆候をいち早く捕捉するという一連の取組みです。

3. サイバーリスク対応戦略の指針

上述のとおり、これからのサイバーリスク対応においては、経営層が自社にとってのサイバー脅威を理解し、積極的に関与することでステークホルダーへの説明責任を果たすとともに、組織内部におけるサイバーリスク対応のあり方を明確に示す必要があります。最後にそのサイバーリスク対応戦略の指針となる3つの施策を提示します。

(1) マネジメントKPI

経営層が組織のサイバーリスク対応状況を監督するためには、一元的かつ直感的に理解する仕組みが必要です。たとえば、バランスト・スコアカード（BSC）による業績評価のように、組織内のサイバーリスク施策をいくつかの領域に分類し、それぞれにおける活動内容にKPI（Key Performance Indicators:業績評価指標）を設けて管理する手法が効果的かつ効率的と考えられます。

KPMGでは、組織におけるサイバーリスク対応領域を6つに分類したフレームワークに基づき、定量的なマネジメントKPIを設定することで、経営層がサイバーリスク対応に積極的に関与できる仕組みの構築を推奨しています（**図表6、7**参照）。

図表7　サイバーリスクマネジメントKPIの例

対応領域	マネジメントKPI(例)
リーダーシップとガバナンス	■IT予算全体に占めるセキュリティ予算の割合 ■リスクアセスメントによる深刻度ごとの指摘事項数
組織体制と人的管理	■セキュリティ教育の参加者数と理解度 ■セキュリティインシデントの発生数
情報リスクマネジメント	■リスクアセスメントの実施回数 ■ハイリスク業務にかかわる委託先数
危機管理とレジリエンシー	■ミッションクリティカルなビジネスプロセスごとの危機管理計画の有無 ■インシデント対応訓練の実施回数
テクノロジーと運用保守	■資産価値を考慮したセキュリティ脆弱性の数 ■セキュリティアラートの発生数と対応数
法令とコンプライアンス	■内部監査による指摘事項の数 ■法規制に関する未解決または未対応事案の数

図表6　KPMGサイバーリスクマネジメントフレームワーク

(2) サイバーインテリジェンス

組織が最適なサイバーリスク対応施策を打つために必要な、真の意味でのサイバー脅威の可視化を実現するためには、「サイバーインテリジェンス」機能の整備が不可欠です（**図表8**参照）。サイバーインテリジェンスとは、外部のセキュリティ専門機関や第三者セキュリティ調査機関、セキュリティベンダーから提供される知見や様々な公開情報（OSINT: Open Source INTelligence）の収集や解析、組織内のセキュリティ監視センター（SOC: Security Operation Center）での分析情報やネットワークトラフィックの統計、セキュリティ脆弱性診断の結果、インシデント対応を通じて得られた教訓の整理など、組織を取り巻くサイバー脅威を文字通り可視化し、対策の高度化に役立てる取組みです。

さらに、昨今では業界間でサイバー脅威動向などの利害が相反しない範囲で情報を共有する枠組みとして、「ISAC（Information Sharing and Analysis Center）」という協議体を設立し、自社だけでは収集・分析しきれない作業を分担しあうことでサイバー脅威に対する知見を高める活動も、国内の金融業界や情報通信業界で始まっています。

経営層は組織がこうした機能を整備するために必要な経営資源を付与するスポンサーシップを提供する必要があります。

図表8　サイバーインテリジェンス機能イメージ

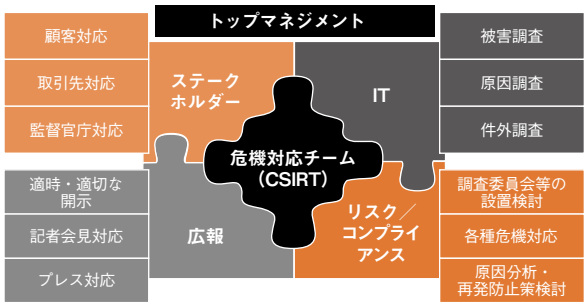
(3) サイバーレジリエンシー

「サイバーインテリジェンス」がサイバー脅威情報をプロアクティブに集積・解析することで先手を打つ“攻め”のサイバーリスク対応戦略とするならば、「サイバーレジリエンシー」は組織がインシデント発生に備えて態勢と対応能力を整え、被害の拡大を防いでビジネスの早期復旧を実現するリアクティブな“守り”の戦略であると言えます。

「サイバーインテリジェンス」機能によって対策を高度化したとしても、完全にすべての脅威を予測し、侵入を防止することは困難であるため、「サイバーレジリエンシー」と併せた“攻め”と“守り”の両翼が機能してはじめて組織のサイバーリスク対応能力を高みに持っていくことができます。

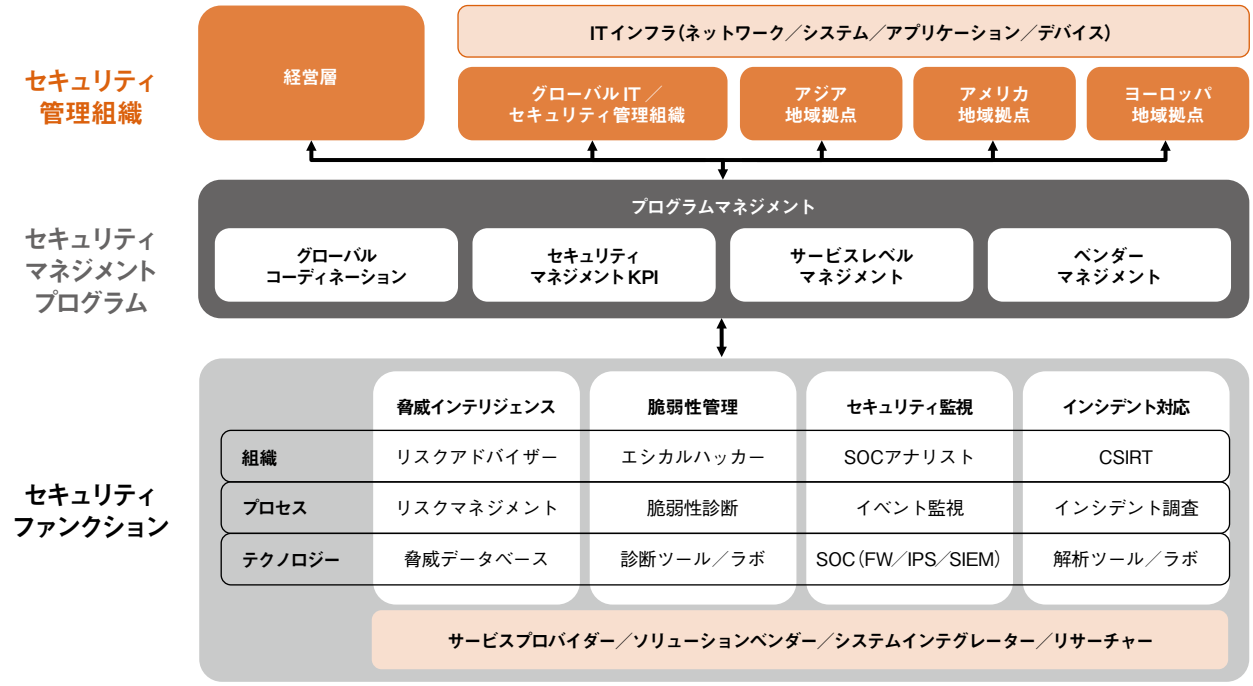
インシデントの発生とその対応が経営責任問題に発展するリスクとなるこれからの社会では、既に多くの企業が構築や検討を進めているCSIRTの設置はもとより、経営層がステークホルダーへの説明責任を果たすための迅速かつ的確な状況把握と報告を可能とする体制や仕組みづくりが不可欠です。企業によってはインシデントの収束や原因究明といった技術的な対応や調査だけでなく、ステークホルダーやメディア、当局への報告や対応、再発防止策の検討など、インシデント発生後に早期にビジネスを回復するための一連の機能を集約した危機対応チームがCSIRTと一体化して対処にあたる態勢を整備しているケースもあります（**図表9**参照）。

図表9　サイバーレジリエンシー機能イメージ



KPMGでは、組織が「サイバーインテリジェンス」と「サイバーレジリエンシー」機能を整備し、「マネジメントKPI」を通じてその効果測定をしながら効率的にサイバーリスク態勢を維持向上していくために、「STIC（Security Threat Intelligence Center）」というフレームワークを独自に開発し、グローバルで提供を行っています（**図表10**参照）。こうしたフレームワークを参考に巧妙化・大規模化するサイバー脅威に立ち向かい、組織のサステナビリティを高めるために経営層によるイニシアチブのもと、積極的な対応を進められることを推奨します。

図表10　サイバーセキュリティマネジメントフレームワーク



モノのインターネット～私たちはその潜在力を全面的に受け入れるべきか

目次

モノのインターネット（IoT：Internet of Things）は、インターネットの誕生と同様に社会に大きな変革を起こすことが見込まれます。

本レポートでは、IoT時代の幕開けと、それがプライバシー、ビジネス、社会全般にもたらすと思われる影響について、KPMGのサイバーセキュリティ専門家が、対立する見方も交え、それぞれの見解を展開しています。

レポートはKPMGジャパンのウェブサイトからダウンロードいただけます。

http://www.kpmg.com/jp/ja/knowledge/article/risk-advisory-thoughtleadership/pages/internet-of-things.aspx

本稿に関するご質問等は、以下の担当者までお願いいたします。

KPMG コンサルティング株式会社
ディレクター 小川　真毅
TEL: 03-3548-5305（代表番号）
masaki.ogawa@jp.kpmg.com

サイバーセキュリティアドバイザリー
kc-cybersecurity@jp.kpmg.com

KPMGジャパン

marketing@jp.kpmg.com
www.kpmg.com/jp