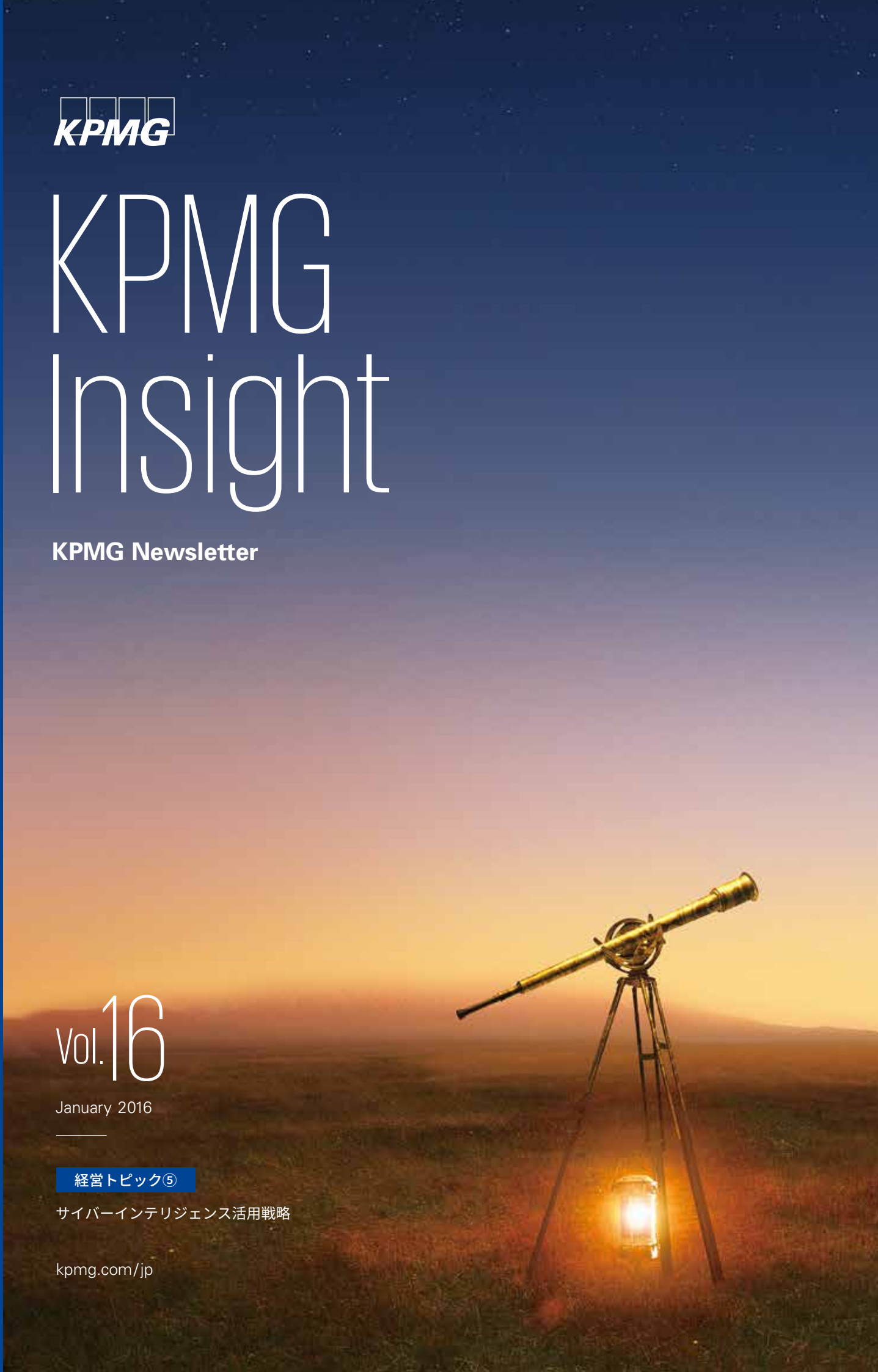
KPMG

KPMG Insight

KPMG Newsletter



Vol.16

January 2016

経営トピック⑤

サイバーインテリジェンス活用戦略

kpmg.com/jp

サイバーインテリジェンス活用戦略

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　真毅
おがわ　まさき

巧妙に作り込まれた標的型メールや、ウェブサイト上の広告を見ただけで感染してしまう悪質なマルウェア、集中的な負荷を与えてシステムやネットワークをダウンさせるDDoS（Distributed Denial of Service：分散型サービス拒否）攻撃など、サイバー脅威は多様化の一途を辿り、その被害はおさまる気配がありません。
こうした状況において、企業の経営者やサイバーセキュリティ責任者は手をこまねいているのではなく、積極的な情報収集と解析作業を通じてサイバー脅威に関する知見の集積と諜報活動（＝インテリジェンス）を推進し、サイバー攻撃リスクを早期に予見することで先手を打ち対策を講じる、という一連の取組みが必要です。
そこで、本稿では、サイバー脅威の変遷と被害拡大の背景を考察し、サイバーインテリジェンスの活用によるサイバーセキュリティ態勢強化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については、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】

- マルウェアのコモディティ化、攻撃手口の複雑化、攻撃表層の拡大といったサイバーリスク環境の変容によりサイバー攻撃被害は拡大基調にあり、組織にとって重大な経営課題となっている。
- 外部の専門機関、内部知見、業界連携を通じて、サイバー脅威に関する様々な知見や兆候に関する情報を得ることができ、組織のサイバーセキュリティ態勢の強化に役立てることができる。
- サイバーインテリジェンスを活用するための戦略、体制、プロセスを整備することで、組織を取り巻く環境変化に伴い生じる新たなサイバー脅威をいち早く捕捉し、リスクの顕在化を未然に防ぐ必要がある。

Ⅰ. サイバー脅威の変遷

「彼を知り己を知れば百戦殆（あや）うからず」。古来より戦略・戦術のバイブルとして世界中で敬重され、いまなお多くの経営者に何かにつけ引き合いに出して語られる、孫子「兵法」における謀攻篇の一説です。これは読んで字のごとく、戦う前に相手のことをよく研究し、自らのこともよく理解していれば、おのずと勝利するための道筋を見出すことができ、敗北することはない、という格言です。

昨今、サイバーセキュリティの分野においては多くの企業や組織が多種多様な手法によるサイバー攻撃の被害を受けており、ステークホルダーからも組織のサステナビリティに対する重大なリスクとして懸念の声が高まると同時に、経営者が果たすべき説明責任の1つとしてサイバーリスクが挙げられるようになってきました。

なぜここまでサイバー脅威が猛威を振るうようになったのか、まずはその変遷について見ていきます。

1. マルウェアのコモディティ化

「Free Trial（お試し無料）、平日9時～17時 電話・メール問い合わせ受付」、これはどこかのパッケージソフトウェアの宣伝文句ではありません。マルウェア作製業者がアンダーグラウンドマーケット上で展開しているキャンペーンの文面です。

世界最初のコンピュータウイルスが何かという話には諸説ありますが、1988年に米国の大学院生が作製した「Morris Worm」と呼ばれるプログラムがそれにあたると言われています。それから四半世紀以上が経ち、コンピュータウイルスは様々な形態に派生しているため、すべてを総称してマルウェアという呼び方が一般的となり、いまでは1日に数万～数十万ものマルウェア亜種が発見されるようになりました（**図表1**参照）。

従来、悪意のあるプログラマーが1つ1つ手製していたマルウェアは、汎用的なツールを利用することで誰でも簡単に製造可能なコモディティ（普及品）と化し、攻撃者たちはさらに高度で巧妙な攻撃手法の作製に時間を割けるようになりました。これはさながら18～19世紀に英国で起きた産業革命のように、機械化による大量生産と、それによって産み出された時間を活用した付加価値の追求という変革に重ね合わせることができ、サイバー脅威の産業革命と言っても過言ではないかもしれません。

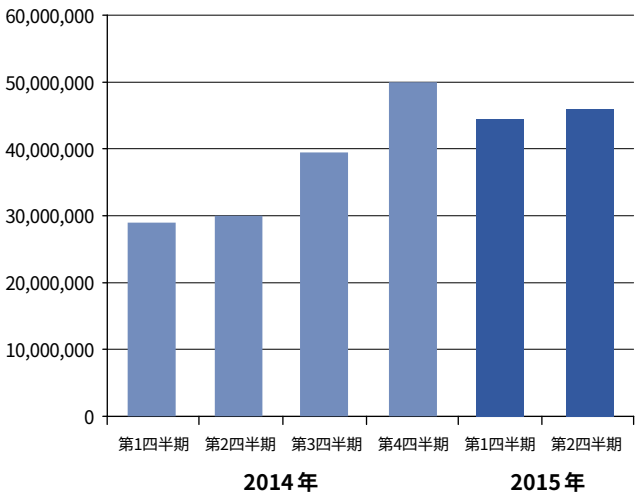
2. 脅威の複雑化

そのサイバー脅威における産業革命の成果の現れが、標的型攻撃や水飲み場攻撃に代表される、巧妙に仕組まれたサイバー攻撃手法です。標的型攻撃は、2015年5月に行政機関で発生した100万件規模の個人情報漏えい事件などを契機として、いまや説明の必要がないほど幅広く認知されるようになりました。

標的型攻撃に使われるなりすましメールは、事前に周到な予備調査を通じてターゲットの組織や従業員に関する情報を収集したうえで作成されているため、日常的に発生する業務上のやり取りと見分けがつかないほど精巧に作り込まれています。さらに、電子メールの仕組み上の根本的な欠陥である、送信元アドレスのなりすましが可能という問題もあり、受け取った電子メールが本物かどうか見極めることは非常に困難になってきています。

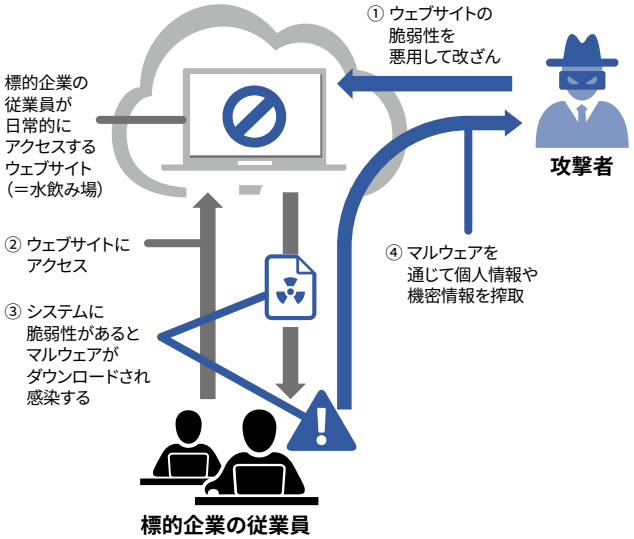
この標的型攻撃と肩を並べるように最近その脅威が問題視さ

【図表1　新たに発見されているマルウェア数の推移】



出所：「McAfee Labs 脅威レポート」（2015 年 8 月）を基に KPMG が作成

【図表2　水飲み場攻撃の手口】



れているのが、水飲み場攻撃です。水飲み場攻撃は、標的とする組織に対して直接的に攻撃を仕掛けることが困難な場合に、その標的組織の従業員が業務でアクセスする可能性がある外部のウェブサイトに対して攻撃を仕掛けて改ざんし、そのウェブサイトにアクセスした標的組織の従業員を、あらかじめ用意しておいた別の悪意のサイトに誘導することによってマルウェアに感染させたり、不正に機密情報や個人情報を入力させて収集したりする手口です(**図表2**参照)。

この手法は、標的組織の従業員を休憩がてら水飲み場に誘い出し、そこで罠にかけるイメージであることから、水飲み場攻撃と言われています。この攻撃も、改ざんしたウェブサイトは一見本来の正当なウェブサイトと区別がつかないようになっており、URLにも変更がないため気づくことが難しく、被害が広がっています。

3. 攻撃表層の拡大

このようにマルウェアや攻撃手法が多様化、複雑化を遂げている一方で、企業や社会のITネットワーク環境も変化し続けています。特に、企業はビジネスの拡大に伴ってITインフラを拡張しており、その範囲は増え続ける傾向にあります。

たとえば、新興国をはじめとした海外で新規事業を立ち上げる場合や、企業を買収した場合などは、ITインフラの統合よりもビジネス活動を優先することでIT環境がサイロ化し、インターネットとの接続口やネットワークセグメントが必要以上に増加して管理しきれなくなっているケースも見受けられます。

さらに、企業のITネットワーク環境に加えて、従業員が私有のモバイル端末を業務で使用するBYOD(Bring Your Own Device)は業務効率の向上に一役買いますが、企業による管理が難しく、十分なセキュリティ対策が強制されないことによるシャドウIT化(本来のIT環境として管理しきれていない影のIT環境のこと)が問題になるケースもあります。BYOD以外にも、従業員がプライベートで使用しているソーシャルネットワーキングサービス(SNS)やブログなどのコミュニケーションツールを通じて従業員の個人情報や、ひいては企業の機密情報が搾取されてしまう場合もあります。

企業を取り巻くこうした一連のITネットワーク環境の変化は、攻撃者にとってみれば攻撃や侵入の入り口が表面的に拡大したことを意味し、攻撃や侵入の糸口をつかむための情報源も増えていると捉えることができます(**図表3**参照)。

Ⅱ. サイバーインテリジェンスの定義と種類

1. サイバーインテリジェンスの定義

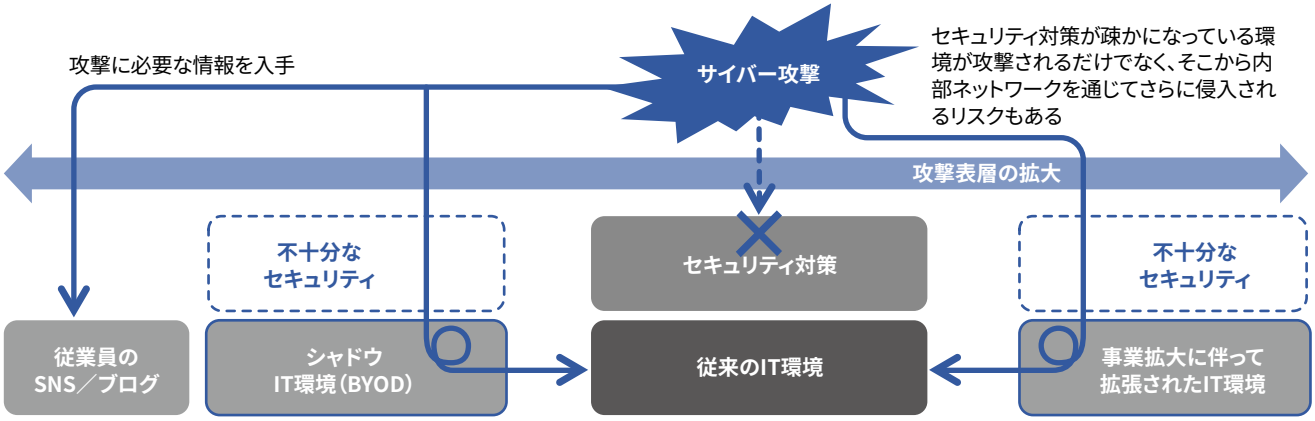
「インテリジェンス」という言葉は元々、軍事活動における概念的な表現であり、敵対組織に関して収集した情報に分析を加えてより高度な示唆を得られるように加工されたもの(諜報情報)、およびそうした活動自体(諜報活動)を指すこともあります。

したがって、「サイバーインテリジェンス」とは、サイバー脅威の発生源や攻撃元、攻撃の手口や兆候などの情報を収集し、分析を加えることで自組織にとってのリスクやそれに対する方策を明確に理解するために集積された知見およびそうした知見を得るための一連の取組みであると言えます。

2. サイバーインテリジェンスの種類

「ビッグデータ」という言葉に代表されるように、世の中には情報が溢れ返っています。膨大な情報の渦のなかから真に有

【図表3　攻撃表層拡大のイメージ】



意義なものだけを見つけ出すのは容易ではありませんが、少しでも効率的に情報を収集するためには、アプローチ可能な情報源とそこから得られる情報の種類を整理しておく必要があります。

ここでは、サイバーインテリジェンス活動を効率的に進めるためのフレームワーク（**図表4**参照）に基づいて、典型的な情報源と主な情報の種類を示します。

（1）外部ソース

一口にサイバー脅威と言ってもその情報は多様かつ専門的なものが多く、すべてを組織の内部リソースだけで収集することは不可能です。実際に、既に多くのセキュリティ専門会社や第三者的セキュリティ調査機関、研究機関、各種セキュリティベンダーが、それぞれの得意分野における専門的な知見を収集しており、こうした情報源から提供されるオープンソースのインテリジェンス（OSINT：Open Source Intelligence）を入手することは、極めて効率的かつ効果的な取組みと言えます（**図表5**参照）。

（2）内部知見

オープンソースインテリジェンス（OSINT）は、ほとんどの場合無償で入手でき、幅広いサイバー脅威に関する動向を理解できるメリットがありますが、それぞれの組織における固有のサイバー脅威までは情報として得られるわけではありません。

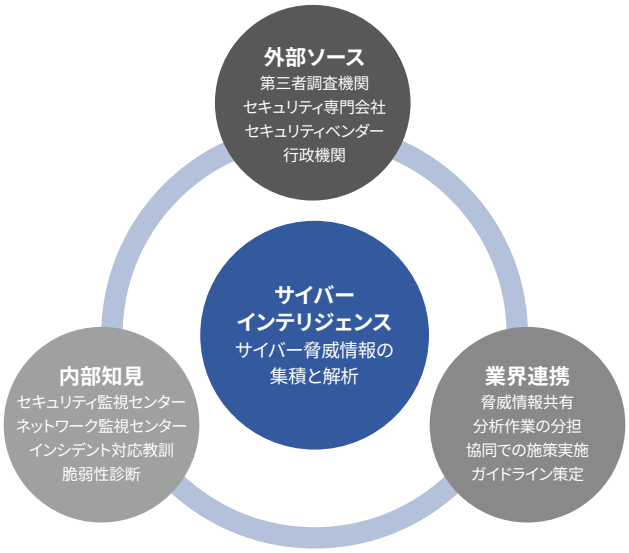
実は、組織がいままさに直面しているサイバー脅威の兆候を炙り出すために有効な情報源が、組織の内部やその取組みのなかに数多く存在しています。たとえば、ネットワークのトラフィック（通信の中身）を分析するだけでも、平常時とは異なる特殊な通信の傾向が見つけ出せたり、組織が保有する情報資産の価値を評価することで最も狙われやすい情報資産（いわゆるCrown Jewel：王冠）やそこに辿り着くための攻撃ルートを特定できたりします。

そのため、近年では多くの組織でセキュリティ監視センター（SOC：Security Operation Center）の設置や検討が進んでいるほか、組織内の情報資産の洗い出しや攻撃ルートの特定、実際に攻撃が可能かどうかの疑似的侵入テスト（ペネトレーションテスト）などの取組みが、専門家による支援のもとで行われるようになってきています（**図表6**参照）。

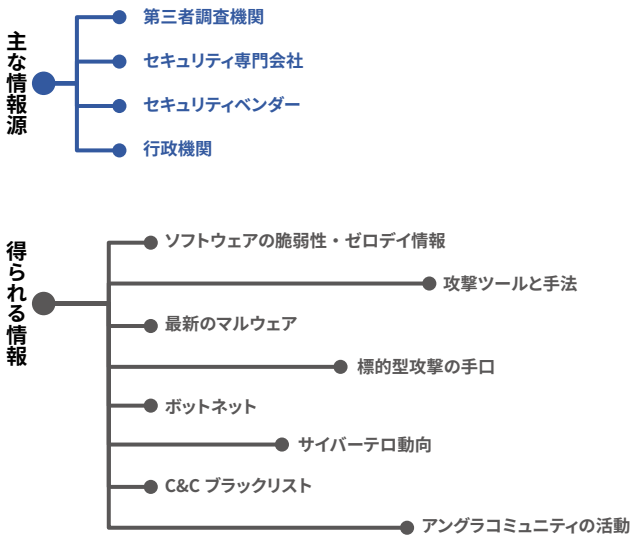
（3）業界連携

外部ソース、内部知見に並ぶ第三のサイバーインテリジェンスとして、自社が所属する業界内での知見の共有が挙げられ

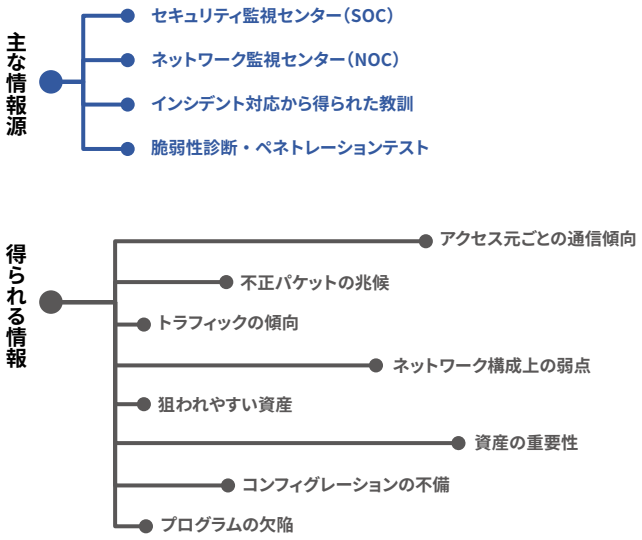
【図表4　サイバーインテリジェンス・フレームワーク】



【図表5　オープンソースインテリジェンス（OSINT）】



【図表6　内部知見に基づくサイバーインテリジェンス】



ます。業界内の連携は、ともすれば同業他社に対してノウハウや営業機密を明け渡すことにも繋がりかねないため、従来はなかなか積極的な活動が行われてきませんでした。しかしながら、昨今のサイバー脅威の隆盛を鑑み、特に政府がサイバーセキュリティ基本法とその解釈を通じて重要インフラ分野と位置付けられている業界（**図表7**参照）においては、その所管省庁が旗振り役となって業界内での横の連携を強める動きが出てきました。

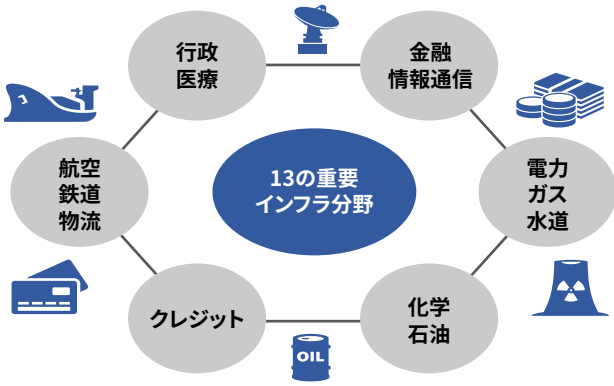
たとえば、特定の業界に所属する企業間で自社が把握しているサイバー脅威動向や攻撃の発生事例など、利害が相反しない範囲で情報を共有する枠組みとして、「ISAC（Information Sharing and Analysis Center）」という協議体を設立し、自社だけでは収集・分析しきれない知見の共有と活動の分担をしあうことで、業界全体としてサイバー脅威への対応態勢を強化する取組みが既に国内の金融業界や情報通信業界で始まっています（**図表8**参照）。

Ⅲ. サイバーインテリジェンス活用戦略

ここまで見てきたように、いまやどこからどのようなサイバー攻撃が発生するか予測することは非常に難しい情勢になっているものの、受け身に回っているばかりではサイバー攻撃による被害を防ぐことはできません。

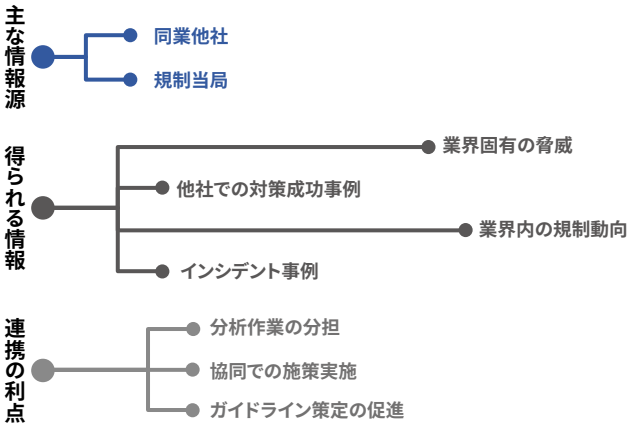
サイバー脅威全盛のこの時代に、組織がセキュリティ態勢を強化するためには、サイバーインテリジェンスを駆使して先手を打ち対策を採る「攻め」のサイバーセキュリティ戦略が必要で

【図表7　重要インフラ分野】

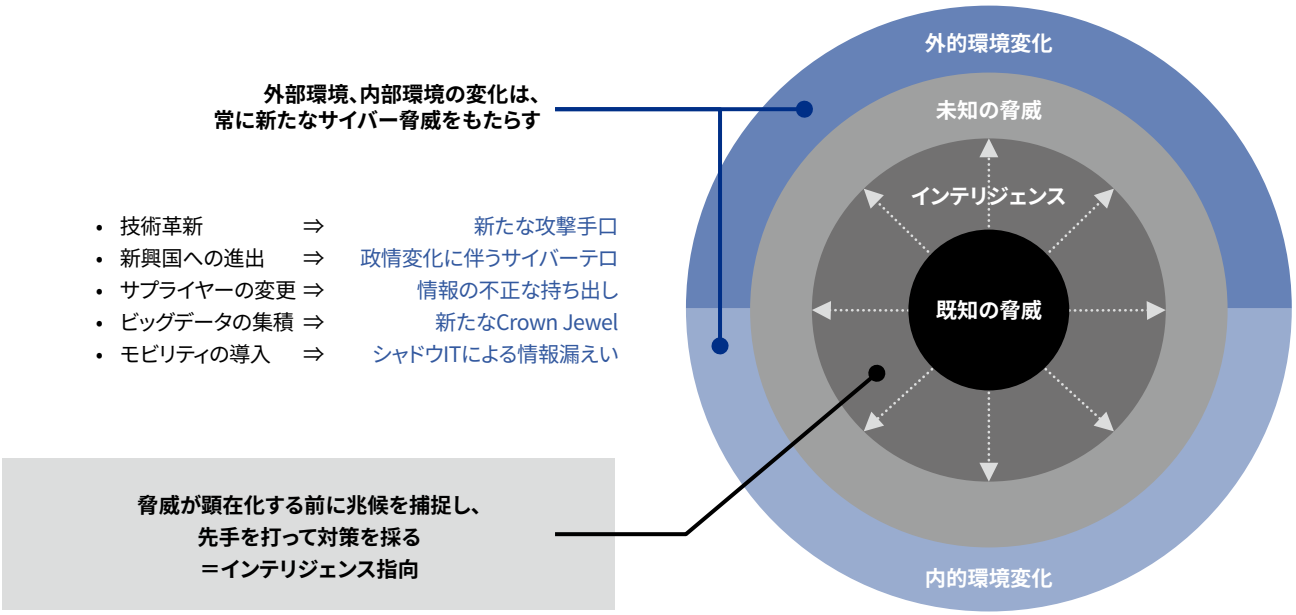


出所：「重要インフラ防護に対する考え方」（内閣サイバーセキュリティセンター）を基にKPMGが作成

【図表8　業界連携によるサイバーインテリジェンス】



【図表9　インテリジェンス指向への切り替え】



す。実際にサイバーインテリジェンスを活用した戦略とはどのようなものか、本章で解説します。

1. インテリジェンス指向への切り替え

組織がビジネス活動を進めるなかでは、必ず何らかの環境変化が発生します。この変化は外的なものと内的なものの2つに大別されますが、どのような変化であれ、ほとんどの場合それらは組織にとって新たな脅威とリスクをもたらします。

たとえば、外的な環境変化の1つとしてIoT（Internet of Things: モノのインターネット）に代表される技術革新が挙げられますが、これは社会や企業にとって様々な利便性やビジネスチャンスを創出する一方、サイバー攻撃の大規模化や新たな攻撃手口の開発など、従来とは異なるサイバー脅威を産み出します。

新規事業の立ち上げや企業買収はドラスティックなビジネス拡大戦略として有効ですが、これまでとは違う新たな利害関係者を創り出し、信用の失墜を狙ったサイバー攻撃を受けるリスクが高まる恐れもあります。

いま経営者には、こうした組織を取り巻く様々な環境変化に伴い発生する新たな脅威に目を向けて、今後起こり得る潜在的な脅威の兆候をいち早く捕捉し、脅威が顕在化する前に先手を打って対策を施すことでサイバー攻撃被害の発生を未然に防ぐ「インテリジェンス指向」へと、マインドの切り替えが求められています（**図表9**参照）。

2. サイバーインテリジェンス活用プロセスの確立

組織がサイバーインテリジェンスを実際に活用できるようになるためには、戦略、体制、プロセスの整備と融合が不可欠です。

まず、大前提として組織が何をどのように守るのかという方針が必要であるのは言うまでもありませんが、明確な目的と活用プロセスなく闇雲に集積してもサイバーインテリジェンスは無用の長物でしかありません。そのためどの情報源からどのようなインテリジェンスを収集するのか、それを誰がどうやって解析するのか、そこから得られた知見に基づく対策の導入に責任を持つのは誰か、といった一連のプロセス構築が必要です（**図表10**参照）。

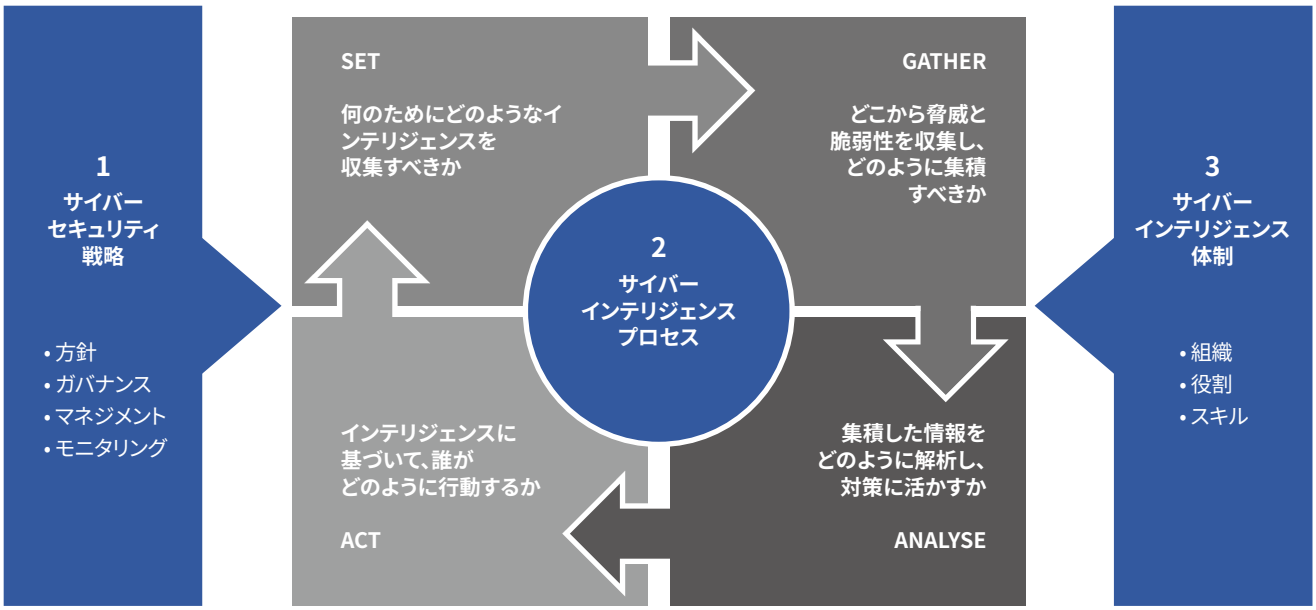
さらに、サイバーインテリジェンスを有効活用するためには、高度な専門知識を有する要員が十分な時間をかけて集積と解析にあたる必要があるため、そうした体制の整備について経営者がスポンサーシップを発揮することも重要です。

3. 意思決定プロセスへの組込み

サイバーインテリジェンスを組織のサイバーセキュリティ戦略に組み込むということは、一連のプロセスを通じて得られた知見が戦略上の意思決定に直接的な影響を与える要素として価値のあるものになって、初めて実現されます。

そのためには、できる限り組織にとって身近な脅威となり得る情報を的確に収集し、組織の現状に照らして固有のサイバー攻撃シナリオとして仮説検証したうえで、重大なリスクが顕在

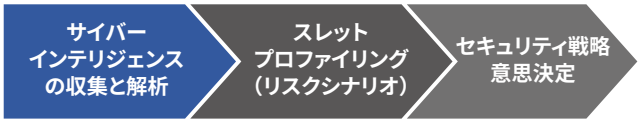
【図表10　サイバーインテリジェンス活用プロセス】



化する可能性の高いシナリオを見出すプロファイリング作業が必要です。

そのうえで、優先的に対処すべきシナリオにできるだけフォーカスして、そのシナリオの発生を防ぐことができるよう、または発生しても大きな被害を受けないように、必要な経営資源の割り当てを行うための意思決定を下すことで、サイバーインテリジェンスが組織のセキュリティ態勢の強化において高い効果を発揮することになります(**図表11**参照)。

【図表11　インテリジェンスの意思決定プロセスへの組込み】



- 攻撃元、手口、経路、標的の資産など、脅威と脆弱性情報を収集する
- リスクシナリオベースのセキュリティ施策の成否は、こうした各コンポーネントの網羅性や精度に強く依存する

- サイバーインテリジェンスに基づき、攻撃側の視点に立って、自社に固有のシナリオを見つけ出す
- 無数にあるシナリオをすべて仮説検証することはできないため、クリティカルな情報資産、ビジネスプロセスにフォーカスする

- リスクシナリオに基づき、対策の優先度と必要な経営資源(費用、人的資源、時間)の割り当てを行う
- 常に変化するビジネス環境に応じて、インテリジェンスの収集と解析、スレットプロファイリングの実行を指示する

【バックナンバー】
サイバーリスク最新トレンドと対応戦略
(KPMG Insight　Vol.15/Nov 2015)

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
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