2023年 Cyber IQ調査

インテリジェンス活用による ダイナミックな セキュリティ対策への転換

pwc

目次

はじめに

現在、「不確実性の時代（VUCA）」という言葉が示すとおり、将来の先行きが見え難く変化の激しい社会を迎えています。この影響は、現実社会に留まらずサイバー空間においてもさまざまなリスクを生み出しており、ときにはインシデントという形で顕在化しています。

このようなリスクの高まりに応じて、企業のセキュリティ投資も増加の一途をたどっています。限りある経営資源の中で投資対効果の高いセキュリティ対策を実現するためには、サイバーインテリジェンスの活用は欠かすことのできないテーマとなります。

本レポートでは前回調査で提唱した「機先を制するセキュリティ」から歩を進め、サイバーインテリジェンスをいかに企業のセキュリティ戦略に統合すべきかを考察します。本稿が日本企業の皆さまがセキュリティ対策を講じるうえでの一助となれば幸いです。

PwC Japanグループ　サイバーセキュリティリーダー
PwCあらた有限責任監査法人　パートナー
綾部 泰二

PwC Japan 合同会社　パートナー
外村 慶

「2023年 Cyber IQ調査」について

日本の広範な産業セクターにおける、企業のセキュリティ組織のリーダー、意思決定権者を対象に調査を行い、260名の回答を得ました。当調査は、2022年6月にPwC Japanグループが実施しました。

第1章

日本企業のサイバーセキュリティを取り巻く変化

継続するランサムウェア被害と従来のサイバークライムへの回帰

ランサムウェアは2022年も依然として猛威を振るっています。独立行政法人情報処理推進機構（IPA）が毎年公開する「情報セキュリティ10大脅威」によると、2021年に続き組織においての脅威の1位に「ランサムウェアによる被害」が挙がっています。

これは「2021年 Cyber IQ調査」でも触れたように、暗号化したファイルの復号のための身代金要求だけでなく、窃取した個人情報や機密情報を流出させることに対しての身代金要求を行うなど、より身代金を奪い取るための手段が悪質化されており、それに応じて攻撃者が金銭を継続的に得ることに成功していることが起因と考えられます。

また、「ランサムウェア・アズ・ア・サービス（RaaS）」など、**自らランサムウェアを用意しなくてもランサムウェアを使った攻撃ができるサービスの台頭により参入障壁が下がっていることも要因**と考えられます。

ランサムウェアによる継続的な被害が出ている一方で、ランサムウェアを用いずに組織内部のネットワークに侵入し、個人情報や機密情報を窃取したうえで、流出させることに対しての**身代金要求を行う恐喝も再び増加しています。**

例えば、US-CERT（米国国土安全保障省配下の情報セキュリティ対策組織）も報告している脅威アクター「Karakurt」は、ランサムウェアを使わずに組織内部から窃取した情報の公開やダークウェブでの競売にかけることをもとに脅迫することが知られています。

また、2021年の後半から2022年の前半で大企業への恐喝を行うことで注目を集めた「LAPSUS$」も同様にランサムウェアを使わずに窃取した情報をもとに恐喝を行っていました。

ランサムウェアの流行以前には、これらと同様の窃取した情報による恐喝はサイバークライムの一種として確認されていたものの、ランサムウェアの流行の陰に隠れて目立ちにくくなっていました。

では、なぜ再び増加傾向に転じているのでしょうか？

一因として、**クレデンシャル情報**（ユーザーなどの認証に用いられる情報）を**入手するハードルが下がったこと**が挙げられます。

ダークウェブの市場では「初期アクセスブローカー（IAB）」と呼ばれる、不正に入手した組織のクレデンシャル情報を他のサイバー犯罪者に販売する集団が存在し勢力を拡大しています。販売されているクレデンシャル情報にはRDP（リモートデスクトップ接続）やVPNのアカウント情報、組織で利用するWebサービスのアカウント情報が含まれているため、IABからクレデンシャル情報を購入すれば、その情報を用いて関連した組織の内部ネットワークに簡単に侵入できるようになります。このクレデンシャル情報の流通量の増加およびこれに伴う販売単価の低下により、入手のハードルが下がっているのです。

流通量の増加は、ランサムウェアの流行も影響しています。

ランサムウェアを用いた攻撃では、まず標的のネットワークに侵入する必要があります。新型コロナウイルス感染症（COVID-19）の蔓延以降、リモートワークの増加に伴いRDPやVPNといったリモート接続は攻撃者にとって恰好の標的となりました。IABがこうした状況を受けて不正に入手されたクレデンシャル情報を取り扱い、ランサムウェアを悪用した脅威アクターからの需要に応えることでIABの市場が拡大を遂げました[*1]。

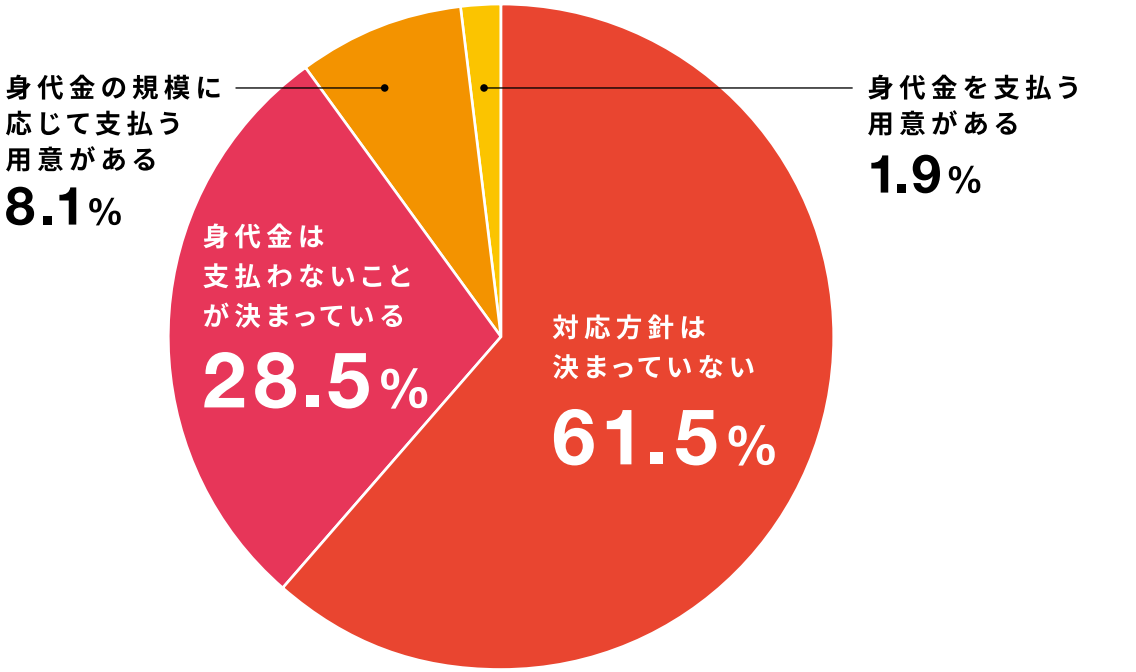
この結果、ランサムウェア・RaaSを用いない脅威アクターにとってもクレデンシャル情報を入手するハードルが下がり、サイバークライムの増加の一因になっていると考えられます。

今回の調査では、ランサムウェアの流行に伴って、従来のサイバークライムへの回帰も発生している中で、サイバークライムにより金銭的要求をされた場合の対応について、各企業がどのように考えているかについて質問したところ、「対応方針が決まっていない」（61.5%）が最も多い回答となりました。**ランサムウェアによる金銭的要求には対応しないことがスタンダードとなっている中で、より広いサイバークライムという単位にはまだ意識が向けられていない**ことが読み取れます。

サイバークライムがこのまま増加すれば、今後、ランサムウェアの対応と同様に金銭的要求をされた場合の対応方針の検討が必要となるでしょう。

［図表1］ **継続するランサムウェア被害と従来のサイバークライムへの回帰**

自組織において、サイバークライムによる情報漏洩が発生した際に、金銭要求の脅迫への対応方針が決まっていますか。（1つだけ／n＝260）



金銭的要求への対応方針だけでなく、予防の観点でも対応が必要となります。ランサムウェアであれば、シグネチャマッチや振る舞い検知による対応も有効でしたが、正規のクレデンシャル情報を用いて侵入される場合には同様の対策は有効となりません。

別の手段として、「アタックサーフェスマネジメント」があります。インターネットなどに外部公開された資産は攻撃者の初期アクセスの対象となり、IABでもクレデンシャル情報が販売されている可能性が高いといえます。

そのため、外部公開された資産のうち、攻撃対象領域となりえる箇所はどこかを把握・管理し、対策します。仮にIABでクレデンシャル情報が売買されたとしても、侵入を許さないようにしていくことが、サイバークライムからも身を守るための1つの有効な手段となるでしょう。

＊1　Palo Alto Networks, 2021, 「ランサムウェア展開に悪用されるRDPプロトコルの解説」
https://www.paloaltonetworks.com/blog/2021/07/diagnosing-the-ransomware-deployment-protocol/?lang=ja

日本の組織に求められる想定脅威アクターのTTPsに基づく対策

「標的型攻撃による機密情報の窃取」は毎年IPAが発表している「情報セキュリティ10大脅威」の組織向け脅威において常に上位に入っている重大な脅威です[*2][*3][*4]。

この脅威は、**機密情報の窃取を主な目的とし、特定の企業や民間団体、官公庁を標的とする攻撃です。**

攻撃が成功した場合、被害は機密情報の悪用による国家の安全保障への影響に留まりません。データ削除やシステム破壊による事業の中断、レピュテーションの毀損、関連組織への攻撃の踏み台として利用されるといった被害も想定されます。比較的最近の事例では、プロジェクト情報共有ツールへの不正アクセスにより、同ツールを利用する顧客企業に影響が及びました。

このような攻撃を防ぐ、あるいは侵入後にいち早く検知するためには、**自組織に対して想定される脅威シナリオを特定し、その戦術、技術および手順（TTPs）に基づいてセキュリティ対策を行う**ことが効果的です。

PwCでは、環境（政治・経済・社会・技術）、脅威アクター（敵対国家、組織犯罪者、ハクティビストなど）、自組織（事業地域、業界、保有資産など）を分析することで脅威シナリオを導出し、関連する情報を監視および検知することで脅威インテリジェンス（対策の提言）を生成し、活用することを推奨しています。

実際に脅威インテリジェンス活動を行う際は、前述したように環境、脅威アクター、および自組織という観点から脅威シナリオを特定しますが、本稿では自組織を「日本の組織一般」として脅威シナリオとその対策を論じます。

脅威シナリオ：日本の組織を標的とする標的型攻撃

PwCでは、日本を標的国に含み、機密情報の窃取を目的として活動する脅威アクターを15のグループとして識別し、追跡しています。これらの脅威アクターは、主に中国および北朝鮮を拠点としています。

中国は「一帯一路（その一環としてのデジタルシルクロード戦略）」および「中国標準2035」などの政策を進めています[*5]。

＊2　IPA, 2020,「情報セキュリティ10大脅威 2020」, https://www.ipa.go.jp/security/vuln/10threats2020.html
＊3　IPA, 2021,「情報セキュリティ10大脅威 2021」, https://www.ipa.go.jp/security/vuln/10threats2021.html
＊4　IPA, 2022,「情報セキュリティ10大脅威 2022」, https://www.ipa.go.jp/security/vuln/10threats2022.html
＊5　PwC, 2020,「ジオテクノロジー（技術の地政学）とサイバーセキュリティ」, https://www.pwc.com/jp/ja/knowledge/thoughtleadership/geo-technology-and-cybersecurity.html

一方、中国を拠点とする脅威アクターはそのような国家戦略に呼応したサイバー諜報活動を実施しています。例を挙げると、「Red Djinn（別名：BlackTech）」は、半導体、人工知能（AI）、ヘルスケア、量子コンピューティング、宇宙・海洋・極地の探索のような特定分野に焦点を当てています。「Red Kelpie（別名:APT41）」は他グループの支援も含め非常に広範な標的を追求しています。また、「Red Vulture（別名：Ke3chang、APT15、APT25、NICKEL）」や「Red Keres（別名:APT31、ZIRCONIUM）」のように、経済戦略的な目的を超えて、公共セクターを標的とするグループも存在します[*6]。

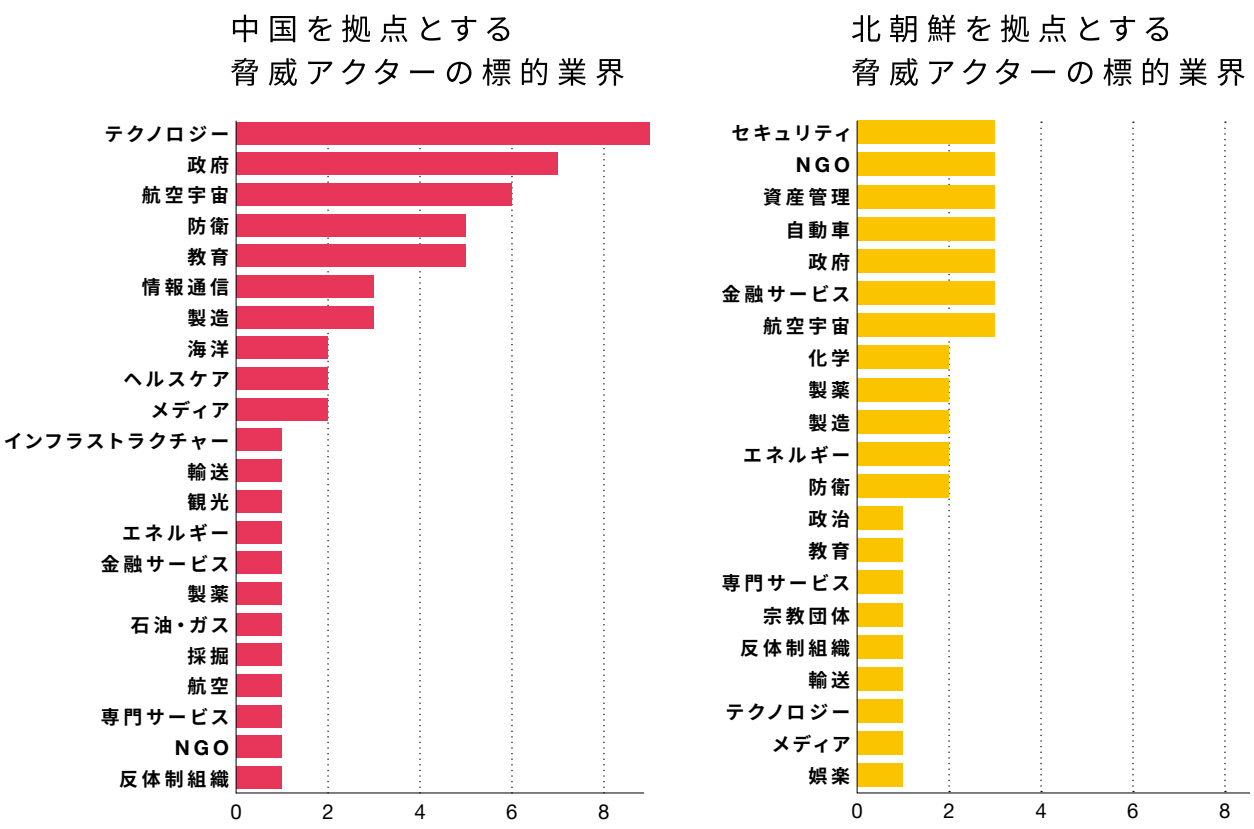
北朝鮮は、核戦力開発の継続が基本戦略です。また、国際的な経済制裁の影響に対処するために、暗号通貨などの資金獲得が求められています。「Black Artemis（別名:Lazarus、Hidden Cobra）」に属し、金銭を目的として活動するサブグループ「Bluenoroff」の後継とみられる「Black Alicanto／Black Dev 2（別名:Dangerous Password、LeeryTurtle）」は、仮想通貨に関わる世界中の組織および金融セクターを標的としています。

一方で「Black Banshee（別名：Kimsuky）」は、政府・公共機関、シンクタンクを含む外交、政策系、研究学術組織（特に原子力研究と国際政策分野）、防衛、航空宇宙、核関連、北朝鮮に関連して活動するジャーナリストやNGOのような市民団体、および宗教団体などの特定の集団を標的としています[*7]。

業界ごとに、当該業界を標的とする脅威アクター数を集計すると、**中国を拠点とする脅威アクターでは、テクノロジー、政府、航空宇宙、防衛、教育（学術界）が上位に入る一方で、北朝鮮を拠点とする脅威アクターでは、資産管理や金融サービス業界が上位に入る**のが特徴だといえます。

これらの業界を事業領域に含む日本の組織は、中国および北朝鮮を拠点とする脅威アクターによる攻撃を脅威シナリオとして想定すべきです。

［図表2］ **国内企業等を狙うAPT（日本企業などを狙う脅威アクター数）**



＊6 PwC, 2022,「サイバー脅威：2021年を振り返る」, https://www.pwc.com/jp/ja/knowledge/thoughtleadership/cyber-threats-2021.html

＊7 PwC, 2022,「サイバー脅威：2021年を振り返る」, https://www.pwc.com/jp/ja/knowledge/thoughtleadership/cyber-threats-2021.html

TTPsの分析と対策

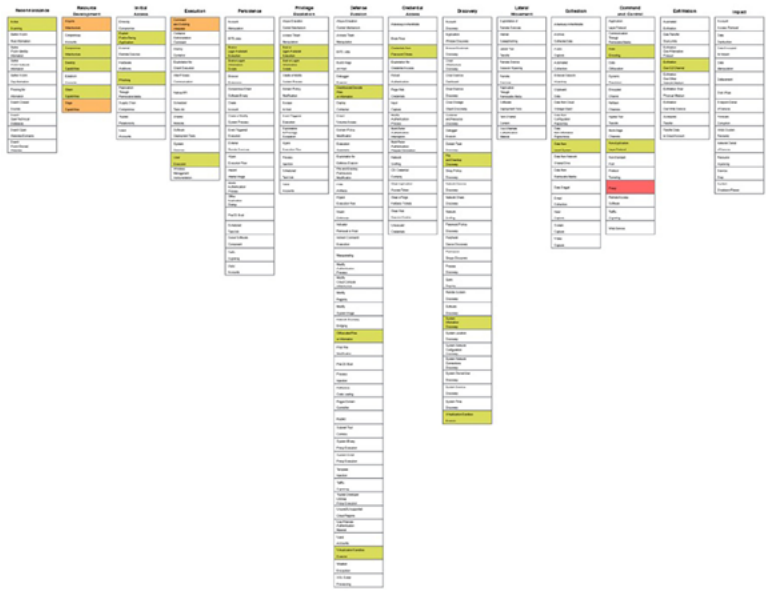
セキュリティ対策は、ISO／IEC27001（ISMS）やNISTサイバーセキュリティフレームワーク（NIST CSF）といった標準・ガイドラインに基づいて実施することが多いですが[*8]、脅威インテリジェンス活動においては米国の非営利団体が作成している攻撃者の戦術・手法に関するナレッジベース「ATT&CK（アタック）」を使用します。これにより、より蓋然性の高い攻撃に焦点を当てた対策が可能となります。

一般に、標的型攻撃ではハッシュ値やIPアドレスのように、変更が容易な指標に基づく検知は困難だとされています。そのため、**脅威シナリオへの対策は、変更がより困難なTTPsに基づいて実施することが合理的**です。ATT&CKでは攻撃手法ごとに回避策、検出方法、およびそのデータソースが整理されているので活用を検討するのがよいでしょう。

次の図は、一例として「Red Djinn（別名：BlackTech）」と「Black Banshee（別名：Kimusky）」について、ATT&CKに基づく攻撃手法を図示したものです。

2つの図を見比べると、脅威アクターによって使用する攻撃手法が異なることが分かります。これが、脅威アクターを具体的に想定し、その攻撃手法に基づいてセキュリティ対策を実施すべき理由です。

［図表3］ 国内企業などを狙うAPT



Red Djinnが使用する攻撃手法
緑黄赤の順で使用が多い

Black Bansheeが使用する攻撃手法
緑黄赤の順で使用が多い

＊8 PwC, 2022,「次世代セキュリティマネジメントモデル～サイバーインテリジェンスを活用したサイバーリスク評価の高度化」, https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/security-management-model2.html

セキュリティ対策を実施する攻撃手法の優先順位付けは、次のような観点で行います。

- 想定脅威アクターの攻撃手法を重ね合わせ、使用頻度の高いものへの対策を優先する
- 自組織のセキュリティ運用体制をATT&CKに基づいてアセスメントし、想定脅威アクターが使用する攻撃手法とのギャップが大きなものを優先する
- 自組織のセキュリティ運用体制をATT&CKに基づいてアセスメントし、採用することでより多くの未対応攻撃手法をカバーできる施策を優先する

本項では、「日本の組織に対する標的型攻撃」という大きな括りで脅威インテリジェンスの考え方を解説しました。各組織においてはより具体的な脅威シナリオに基づいた脅威アクターの特定とその攻撃手法への対策が推奨されます。

ソフトウェアサプライチェーンにおける脅威の高まり
――ステークホルダーごとの考慮事項と取り組み状況

ソフトウェアサプライチェーンにおける脅威のサプライチェーンを悪用した攻撃に代表される、「サイバーセキュリティにおけるサプライチェーンに関する脅威」が高まっています。

実際、2021年に欧州ネットワーク・情報セキュリティ機関（ENISA）が発表している「Understanding the increase in Supply Chain Security Attacks[*9]」では、**サプライチェーンを狙った攻撃は例年に比べて4倍になる**と予測されています。

また、IPAが公表している「情報セキュリティ10大脅威」では、2019年に「サプライチェーンの弱点を悪用した攻撃」が4位にランクインし[*10]、それ以降継続して主要な脅威の1つとして位置付けられています。

ひとえに「サプライチェーンの弱点を悪用した攻撃」といっても、その形態は多岐にわたり、以下のような事例が確認されています。

1. 外部委託先の従業員による不正
2. 外部接続されたシステムを介した不正アクセス
3. SaaSなどの外部プラットフォームの侵害
4. 調達ソフトウェア・システムへの不正コードの混入
5. 自社で利用しているサードパーティソフトウェアの脆弱性を狙った攻撃

こうした攻撃の中でも近年特に注目を集めているのが上記3～5に相当するソフトウェアのサプライチェーンに関する脅威です。

2020年12月、IT管理ツールの開発・販売を行うソフトウェアベンダーが外部から不正アクセスを受け、自社で開発・販売しているパッケージソフトウェアに不正コードが混入されていたことが発覚。混入された不正コードは外部からの不正アクセスを可能にするバックドア機能を有しており、このパッケージソフトウェアは正規のオンラインアップデートの仕組みを介して同社製品を利用するユーザー企業に配布されていました。

このインシデントは、当該ソフトウェアが米国政府関連機関でも広く利用されていたこともあり、大きな反響を呼びました。米国政府は、2021年5月に「国家のサイバーセキュリティの向上」に関する大統領令（EO14028）[*11]に署名し、その中で計画されているさまざまな施策が順次実行されています。

また、2021年12月にはJava用のログフレームワークとして広く利用されているオープンソースソフトウェアである「Log4j」に致命的な脆弱性が発見され、この脆弱性を悪用した攻撃がインターネット全体で大規模に発生しました。

「Log4j」が外部ライブラリとしてパッケージソフトウェア、SaaSなどで広く利用されていたこともあり、ユーザー企業が自社で管理するWebシステムだけでなく、自社で調達・導入しているパッケージソフトウェアや自社が利用している外部のSaaSサービスについても脆弱性の有無、自社への影響を確認・把握しなければならない事態となりました。

＊9　https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
＊10　https://www.ipa.go.jp/security/vuln/10threats2019.html
＊11　https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

各ステークホルダーの取り組み状況

こうした状況を受けて、国・業界団体、ソフトウェアサプライチェーン上のサプライヤー、完成品ベンダー、ユーザー企業といった各ステークホルダーは、さまざまな対策への取り組みに力を入れています。

米国では、前述の大統領令において連邦政府が利用するソフトウェアに関するソフトウェアサプライチェーンの強化に関する施策が要求されています。

具体的には、セキュリティ侵害時のインパクトが大きい「クリティカルソフトウェア」の基準策定、ソフトウェアの開発・調達などを行う際のライフサイクル基準、セキュリティベストプラクティスの整備などです。

また、米国立標準技術研究所（NIST）も2022年2月に「NIST SP800-218 Secure Software Development Framework（SSDF）Version 1.1[*12]」を公開しており、従来提唱されている「ソフトウェア開発ライフサイクル（SDLC）」におけるより具体的なベストプラクティスとして実施すべき推奨対策が整理、提唱されています。

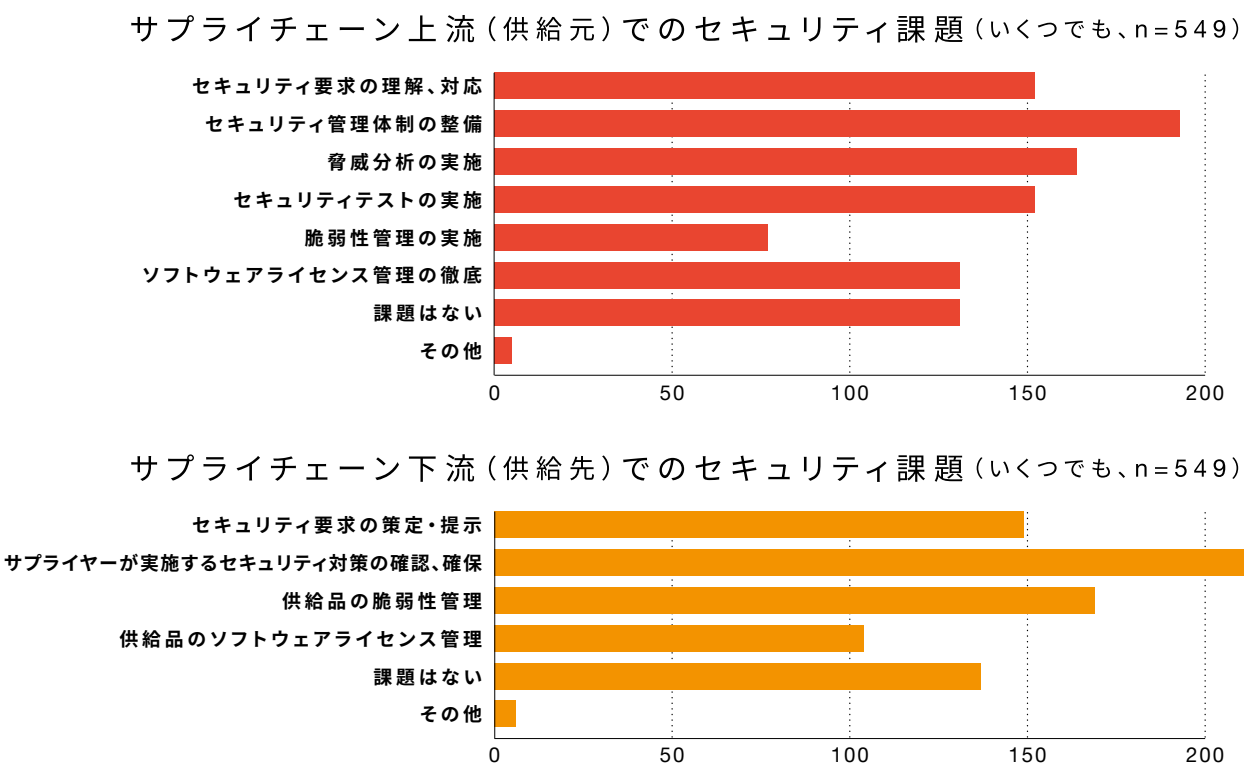
これらの取り組みはガイドラインなどの整備に留まらず、米国政府によってオープンソースサミットが開催され[*13]、さまざまなテクノロジー企業・団体との議論が行われており、今後サービス・製品ベンダーを介してユーザー企業にも波及していくことが考えられます。

サービス・製品などの開発、販売を行う製品・サービスベンダーでもセキュリティ脆弱性は関心事となっており、各社さまざまな対策に取り組んでいます。

PwCが実施した「製品サイバーセキュリティ実態調査[*14]」では、サービス・製品開発に関する企業を跨いだソフトウェアサプライチェーン上の関心事として、サプライチェーン上流（供給元）では「供給先から要求されたセキュリティ管理体制の整備」（35.2%）、次いで「脅威分析の実施」（29.9%）が挙げられています。

一方、サプライチェーン下流（供給先）では、「サプライヤーが実施するセキュリティ対策の確認、確保」（38.4%）、次いで「供給品の脆弱性管理」（30.8%）であり、供給元で挙げられた回答と丁度対応する結果となっています。

［図表4］ ソフトウェアサプライチェーンにおける脅威の高まり



＊12 https://csrc.nist.gov/publications/detail/sp/800-218/final
＊13 https://www.bleepingcomputer.com/news/security/white-house-reminds-tech-giants-open-source-is-a-national-security-issue/
＊14 https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/vulnerability-management-sbom7.html

サービス・製品ベンダーにおける「SBOM」普及の期待

同調査の結果を企業単位で見ると「脅威分析の実施」「セキュリティテストの実施」については約70%がなんらかの取り組みを既に実施している結果が確認されており、各社での対策強化の余地は残るものの、それ以上に企業を跨いだセキュリティ確保、検証が課題になっていくことが予想されます。

こうした状況を受けて、昨今注目されている考え方が「SBOM（Software Bill of Materials：ソフトウェア部品表）」です。

SBOMは、名称のとおり特定製品に含まれるソフトウェアコンポーネント、ライセンス、依存関係などの一覧であり、これをサプライチェーン上流から下流に提供することで、企業を跨いだスムーズな脆弱性管理を実現するものです。

例えば、OSSなどソフトウェアコンポーネントに脆弱性が発見・報告された場合、ソフトウェアサプライチェーン上に存在する各ステークホルダーはSBOMを確認することで、自社が他社から供給を受けているソフトウェア内に脆弱性の影響を受けるコンポーネントが含まれているかどうかを確認することが可能となります。

実際、前述の米国の大統領令においても連邦政府に納入するソフトウェアに関して製品・サービスベンダーによるSBOMの提供について言及されています。

また、自動車業界では既にSBOMの導入・運用が一部開始されています。自動車製造は、OEM（完成品ベンダー）を頂点（サプライチェーン上の最後尾）とする巨大なサプライチェーンとして市場形成されています。

また、2020年に国連欧州経済委員会（United Nations Economic Commission for Europe）の自動車基準調和世界フォーラム（WP29）において策定された自動車のサイバーセキュリティ対応の国連標準である「UNR155」において、サプライチェーン全体を通したセキュリティの確保が義務付けられています。そのためOEM主導でサプライチェーン上の各企業を跨いだ取り組みが推進されやすい環境にあるといえます。

ユーザー企業特有の課題

一方、ITの世界ではサプライチェーン上の最終消費者にあたるユーザー企業で考慮すべき対策は、ソフトウェアの利用形態に応じて異なります。

例えば、パッケージソフトウェアや外部のSaaSサービスを調達・利用している場合、サプライチェーン上で発生した脆弱性などの問題の影響を自社が受けるかどうかはベンダーから公開・提供される情報に基づいて判断、対応することとなります。

これは、従来の脆弱性対応と同様であり、**ITシステムの構成管理データベースを整備し、どこにどのようなシステムがあるのかを把握できる状態を維持する**ことが重要です。

一方、自社または外部インテグレーターなどに委託し、システム開発・運用を行っている場合、システムを構成するコンポーネントを把握し、各コンポーネントのSBOM情報に基づいて対策要否を判断する必要があります。

これを実現するためにはシステムを構成するコンポーネント全体のSBOM情報をデータベース化し、適宜対応要否の判断、修正を行うことになります。

こうした一連の対応をユーザー企業、システム子会社、インテグレーターのいずれが行うのか事前に整理しなければなりません。

特にITの世界ではSBOMの必要性が訴求されてから日が浅く、こうしたシステム開発におけるステークホルダーの役割・責任についても今後検討が必要になるでしょう。

セキュリティ人材の獲得競争

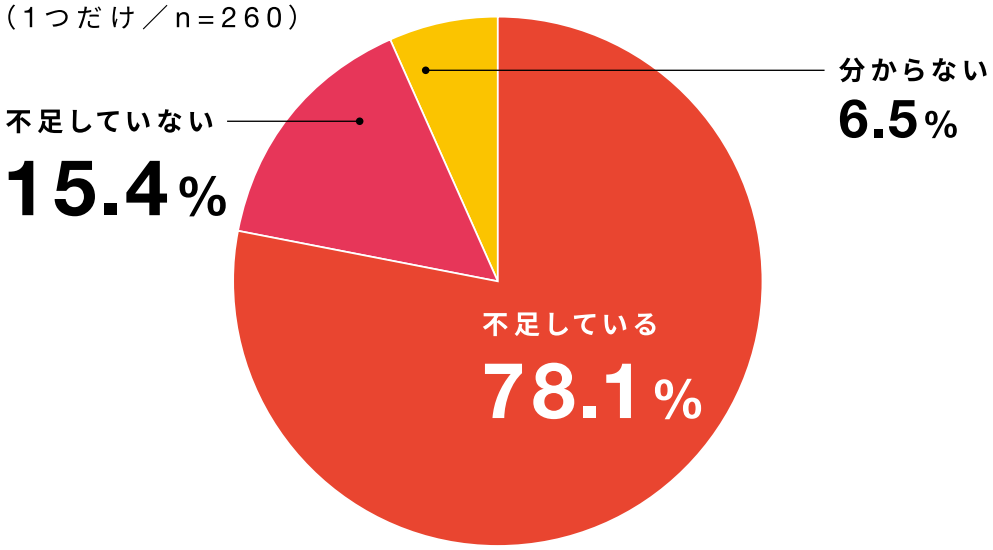
セキュリティ人材に目を向けると、多くの企業では人材不足を実感しており、人材の獲得は容易ではないことが分かっています。

今回の調査では、**78.1%もの回答者が「セキュリティ人材は不足している」と回答。**また、人材獲得時の難しいポイントや不安として、「自組織で活かしきれるかが不明確」(58.5%)、「高い給与」(37.3%)、「応募が少ない」(36.5%) が主な理由であり、自社に合った優秀な人材を獲得するのは一筋縄ではいかなくなっています。

一般的にセキュリティ人材には、幅広いITセキュリティ知識とリスク管理能力、豊富なインシデント対応の経験、経営者とのコミュニケーション能力などが求められます。このように高度なスキルや能力を持ち合わせるセキュリティ人材は獲得が容易ではありませんが、組織が人材の獲得競争において優位な立場を取らなければ、セキュリティ施策の推進が困難になり、レジリエンスを高めることが難しくなるため、早急な対策が必要です。

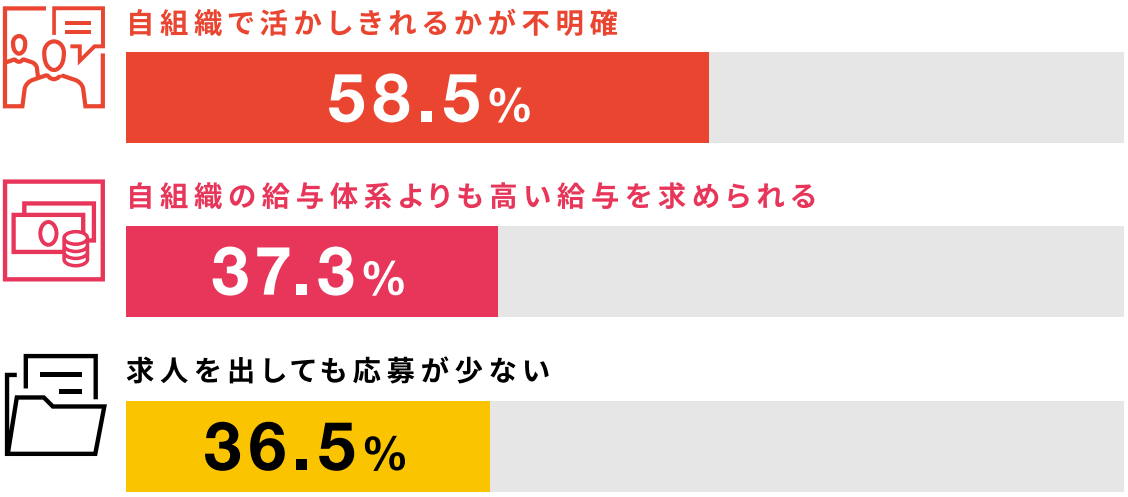
［図表5］ **セキュリティ人材は、約8割の企業で不足している**

貴社において、セキュリティ人材は不足していると感じますか。
(1つだけ／n=260)



［図表6］ **セキュリティ人材の獲得で難しいポイント**

セキュリティ人材獲得時の難しいポイントや不安は何ですか。
(1つだけ／n=260)

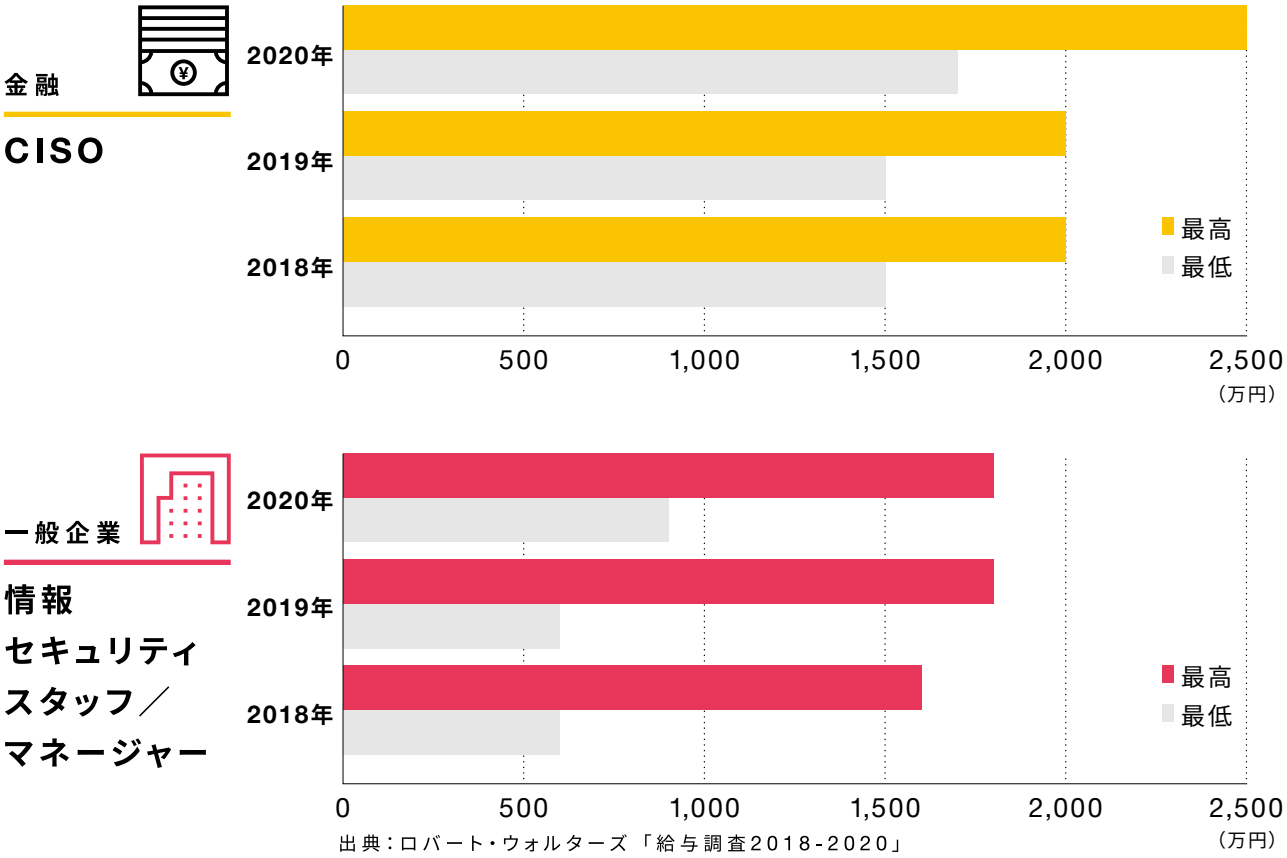


セキュリティ人材の需要に対して、供給できる数が限られているため、給与は必然的に上昇傾向にあります。ロバート・ウォルターズ「給与調査」によると、2018年から2020年の3年間で、金融機関のCISOの給与、情報セキュリティスタッフやマネージャーの給与は大幅に上昇しています[*15]。この給与調査によると、IT人材の給与も高騰しており、セキュリティ人材とIT人材の給与に大きな差はありませんでした。

このような給与高騰に対して、今回の調査で特別な制度を用意しているかと聞いたところ、半数以上（51.5%）が「特に給与体系や手当を用意していない」と回答しています。つまり、**多くの企業は金銭面でのアピールが難しく、限られたカードで人材獲得競争に挑まなければならない状況にある**といえるでしょう。

＊15 出所：ロバート・ウォルターズ,2020,「給与調査2018-2020」,2022/10/26閲覧,
https://www.robertwalters.co.jp/content/dam/robert-walters/country/japan/files/salary-survey/20_JAPAN_Jpn.pdf

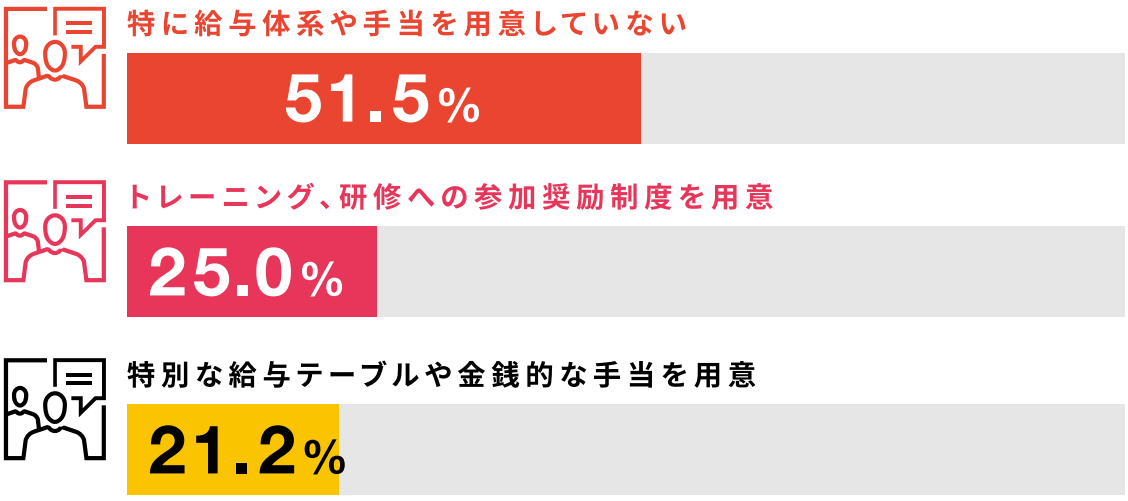
［図表7］ セキュリティ人材の給与は上昇している



出典：ロバート・ウォルターズ「給与調査2018-2020」

［図表8］ セキュリティ人材獲得のために用意している特別な施策

セキュリティ人材獲得のために別途給与テーブルや特別な手当などの制度を用意していますか。（1つだけ／n=260）



それでは、企業がセキュリティ人材の獲得競争で優位な立場を維持するために、どのようなことに取り組むべきでしょうか。

PwCでは、以下の3つの視点をCISOやセキュリティリーダーが持つべきであると考えています。

1. 採用は人事任せにせずに、セキュリティ部門が積極的に関与すべき
2. 給与以外の自社のアピールポイントを明確にすべき
3. 人材獲得戦略を策定すべき

1 採用は人事任せにせずに、セキュリティ部門が積極的に関与すべき

一般的な企業では、セキュリティリーダーは募集要項作成時と面接の段階でしか採用プロセスに関与していません。

しかし、人材不足かつ給与が高騰しているセキュリティ人材の採用は、受け身のスタンスでは成功の果実を得ることは困難です。採用は人事に任せるのではなく、CISOやセキュリティリーダー自らが求める人材像を定義し、応募状況や辞退理由を詳細にモニタリングするなど、採用に積極的に関与しましょう。

2 給与以外の自社のアピールポイントを明確にすべき

特に給与や手当に制約がある企業においては、中長期的なキャリアプランや給与上昇モデル、裁量の拡大、自由なワークスタイルを採用時にアピールすべきです。

また、実際のインシデント対応経験やプロジェクト事例など、自社でないと経験できない業務をアピールすることも有効です。

3 人材獲得戦略を策定すべき

プロアクティブに人材獲得に取り組むために、自社のセキュリティ部門で働くメリットを客観的に分析し、どのような志向の人材に対して、何をアピールするのかを戦略的に策定しましょう。

例えば、次の図「セキュリティ人材獲得の施策例」では、管理職志向・やりがい重視の人材に対して、自社で実施している権限移譲や裁量の拡大をアピールすべきであることが分かります。

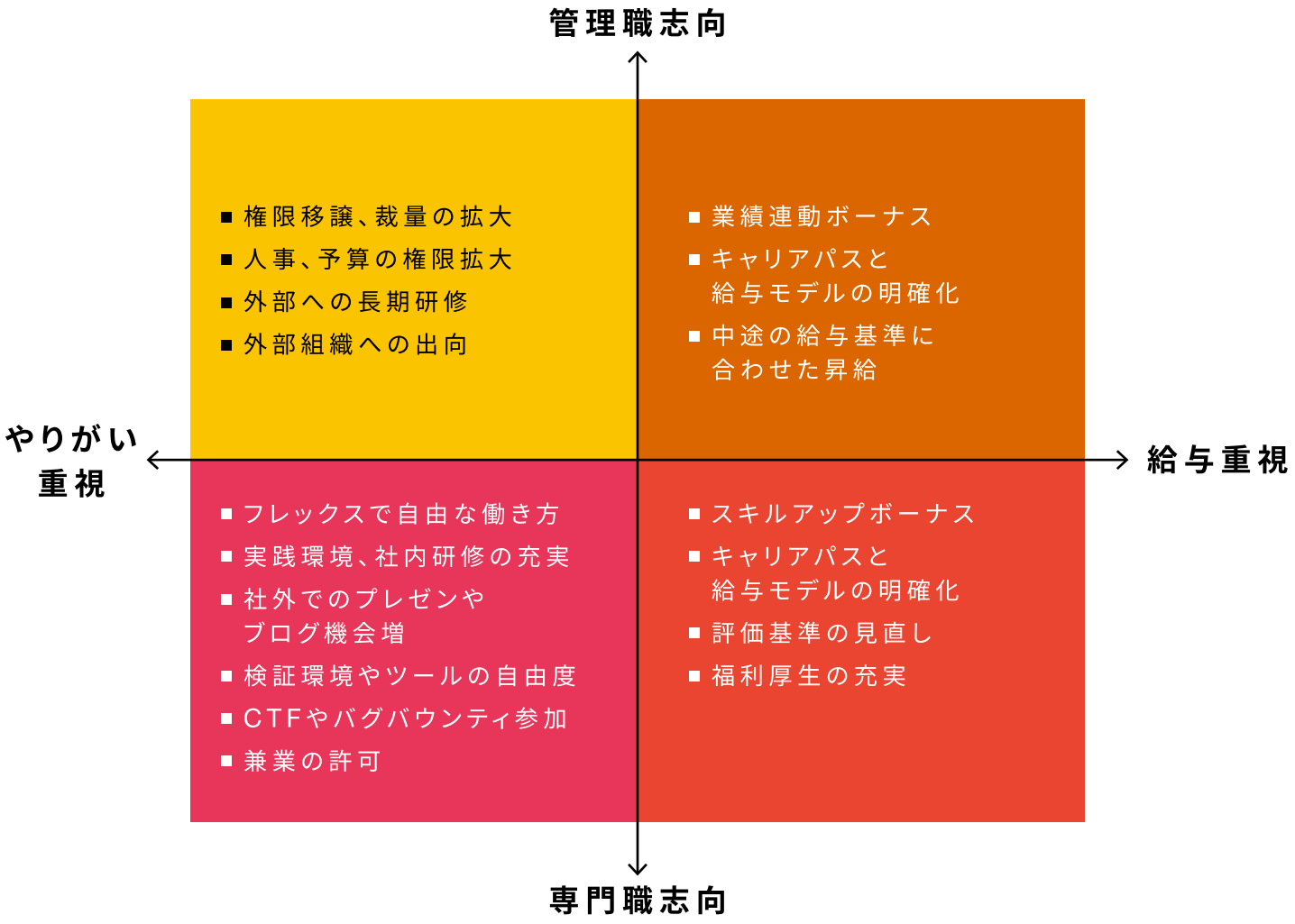
一方、自社が求めていない人材に関する施策の優先度は、かなり低く設定しても問題はありません。

このような人材獲得施策を自社用に整備することは、募集ポジションに対するアピールポイントを明確にするうえで非常に有効です。

これまで述べてきたとおり、セキュリティ人材の獲得競争は激化しており、給与水準も高騰しています。人材獲得を人事任せにするのではなく、CISOやセキュリティリーダー自らが採用戦略を策定し、積極的に関与することが求められます。

本調査では、21.5%の回答者が「セキュリティ人材を育成していたにもかかわらず、より良いフィーやポジション、やりがいなどを理由に他社に転職した経験がある」と答えています。何も手を打たなければ人材は自然減になるという前提に立ち、持続可能な組織を構築することが重要です。

［図表9］ セキュリティ人材獲得の施策例



PwCが定期的に実施しているCISOインタビューをもとにした人材獲得や既存メンバーの引き留め策の例。PwCにて各取り組みを上記の4象限に分類した。なお、個人の志向は、重要視する幅の広さや強弱にばらつきがあり、また時間とともに変化することに留意が必要。

第2章

インテリジェンスを活用したダイナミックなセキュリティ対策への転換

中長期ロードマップ戦略が抱えるセキュリティ投資のジレンマ

企業を取り巻くサイバー脅威が激変している状況の中、政府機関や機関投資家といったステークホルダーからは、サイバーセキュリティ対策強化と情報開示を求める声が高まっています。それはサイバー情報開示に関する各種ガイドラインの変化を見ても明らかでしょう。

例えば、2017年に経済産業省とIPAが公開した「サイバーセキュリティ経営ガイドラインVer2.0」には、「サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である」と明記[*16]されています。

また、2021年に金融庁が改訂した「投資家と企業との対話ガイドライン」には、経営環境の変化に対応した経営判断の指針として、「サイバーセキュリティ対応の必要性など、事業を取り巻く環境の変化が、経営戦略・経営計画等において適切に反映されているか」という文言が盛り込まれています。

さらに、2022年2月に米国証券取引委員会（SEC）が「サイバーセキュリティに関する情報開示を強化する規制」の中に、「サイバーインシデントが発生した場合は、48時間以内に情報を開示しなければならない」と明記[*17]しています。

また、RBC Global Asset Managementが公開した「Responsible Investment Survey 2021（責任投資に関する調査2021）[*18]」によると、機関投資家が懸念しているESG（環境・社会・ガバナンス）のランキングでは、サイバーセキュリティが第2位となった。このことから、機関投資家がサイバー脅威を「企業の価値に対して直接影響を及ぼすリスクである」と捉えていることが読み取れます。

こうした状況で企業は、ステークホルダーに対して説明責任を果たす対策を講じています。

しかし、**その対策が“正しい方向”に向いているわけでは、必ずしもありません。**

一般社団法人日本情報システム・ユーザー協会（JUAS）が2022年4月に公開した「企業IT動向調査報告書2022」によると、3年後の情報セキュリティ関連投資を「増加させていく予定である」と回答した比率は、2021年度で約60%に上っています。ただし、「投資を増やす予定の内訳」を見ると、本当に有効な投資なのかは疑問が残ります。

＊16 https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf
＊17 https://www.bankinfosecurity.com/us-sec-proposes-48-hour-incident-reporting-requirement-a-18493
＊18 https://www.rbcgam.com/en/ca/about-us/responsible-investment/our-latest-independent-research

例えば、セキュリティ関連費用の増額理由を見ると、「新規システム導入やDX（デジタルトランスフォーメーション）の推進施策に対するセキュリティ対策のため」と回答した比率は31%に留まります。

一方、「全システムを横断したセキュリティ対策」は42%、「現行、既存システムに対するセキュリティ対策」は25%です。

つまり、**投資の約70%の費用が、これまでに導入したセキュリティ対策の保守運用や、インフラとして最低限導入しているセキュリティ対策に充てられている状況**なのです。

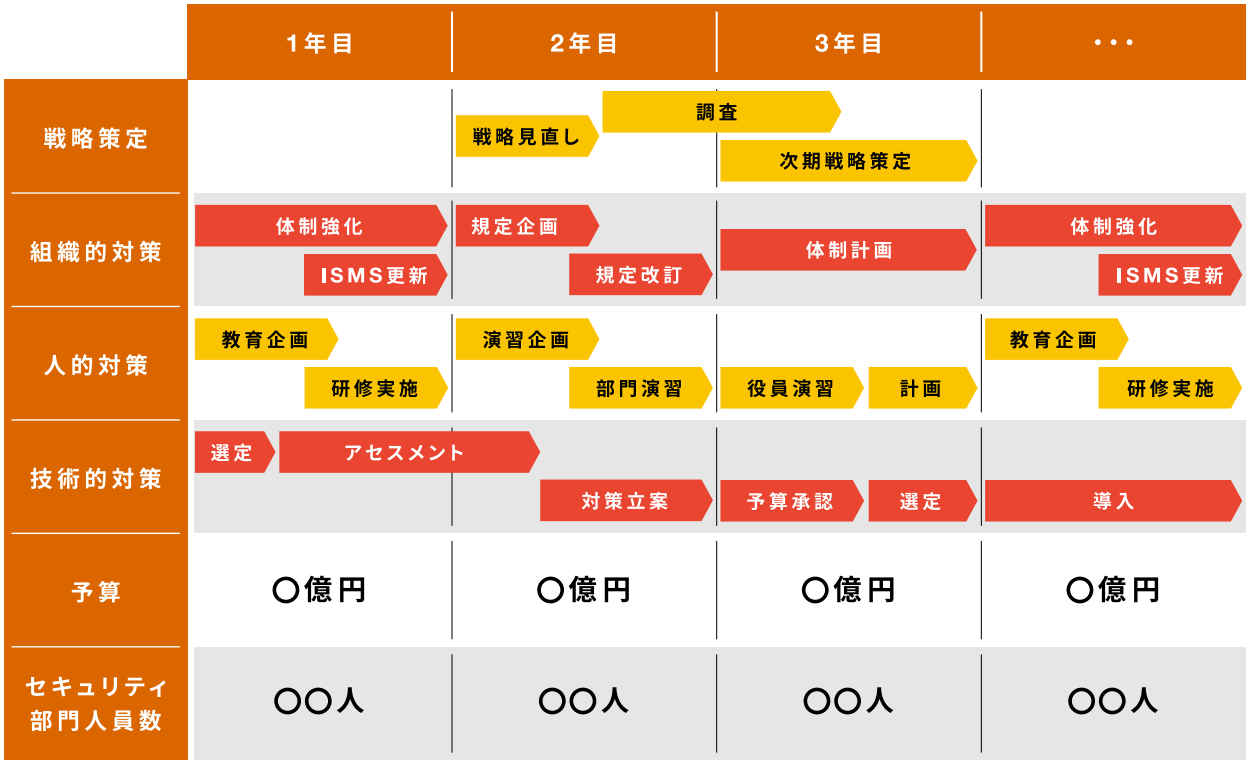
もちろん、こうした投資は「間違い」ではありません。しかし、システムの脆弱な部分を場当たり的に対処した結果、継ぎ接ぎだらけのセキュリティ対策になってしまったり、重複部分が発生したりして、余計な手間やコストがかかってしまうケースは多いといえます。

一般的に企業がセキュリティ投資を行う場合は、中長期のロードマップを策定し、それに沿った戦略を立案します。そのアプローチは以下のようになります。

1. 現状のアセスメント
2. 数年後の目指すべきセキュリティ水準の設定
3. 現行施策とのギャップを識別
4. ギャップを埋めるために必要な投資額や人員構成の算出
5. 目指すべき姿に向けて施策を実行

［図表10］ **セキュリティロードマップの策定・戦略立案が重要**

一般的な企業のセキュリティロードマップ



ただし、このアプローチはサイバー脅威の“進化”に対応できません。戦略策定時のリスクで決定した「目指すべきセキュリティ水準」は、時々刻々と変化するサイバー脅威の前では形骸化してしまいます。

特に定められた年間予算の中では、新たな脅威に対して有効な施策を講じようとしても限界があります。その結果、「運用でカバー」という現場丸投げの状態になってしまい、ただでさえ忙しいセキュリティ担当者は業務多忙で疲弊してしまいます。

誤解のないように付け加えると、中長期のロードマップを描くこと自体を否定しているわけではありません。強調したいのは、**今後は中長期のロードマップを描いたうえで、状況に応じて迅速、かつダイナミックにセキュリティ投資をすることが求められる**ということです。

新たなサイバー脅威の台頭によって、既存のセキュリティ対策が根底から覆されるような状況では、これまでとは違ったアプローチを取る必要があります。そのアプローチの中心となるのが「サイバーインテリジェンス」の活用です。

サイバーインテリジェンス活用、組織のCyber IQを高めるアプローチ

「サイバーインテリジェンス」とは、自組織に発生し得る脅威を予測し、脅威が発生した際に対応できるよう備える活動を指します。

これを実現するためには、第1章でも解説したようにセキュリティ対策に脅威アクターのプロファイルを活用する「脅威インテリジェンス」と呼ばれる取り組みが重要となります。

一方で、サイバーインテリジェンスはこうした技術的観点（Technology）に留まらず、組織がどのようなセキュリティ戦略を採用・実施すべきかといった戦略的観点（Strategy）、セキュリティ運用の設計やその改善・高度化に関する運用観点（Operations）が包含されます。

［図表11］ **サイバーインテリジェンス3つの観点で考える**

企業はこうしたインテリジェンスを活用し、インシデントが発生した場合であっても被害を極小化・最小化し、しなやかにシステムを回復させてレジリエンスを向上させなければなりません。

そのために必要なのが、「組織におけるCyber IQの向上」です。次の図は、過去のセキュリティ戦略とCyber IQの高い組織の戦略立案を比較した表です。

［図表12］ 過去のセキュリティ戦略とCyber IQの高い組織の戦略立案の比較

		今までのサイバーセキュリティ戦略	Cyber IQの高い組織
戦略策定	戦略インプット	過去事例とベンチマーク	サイバーインテリジェンス
	戦略策定時期	戦略策定の前年から	常時
	戦略期間	3年	特に定めない
	予算計画	3カ年予算	3カ年予算＋変動予算
	人員計画	3カ年計画	3カ年計画＋外部活用
対策実行	対策契機	他社事例をもとにした事後対応	攻撃者分析結果による事前対応
	優先度付け	戦略策定時のリスクから決定	サイバーインテリジェンスベースのROIにより決定
	サイバー情報	中	多
	分析時間	中～長	短
	有効性評価	3カ月～1年単位	常時

出所：PwC,2021,「2021年 Cyber IQ 調査」,2022/9/13閲覧,
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/cyber-iq-survey2021.html

Cyber IQの高い企業は、戦略インプットにサイバーインテリジェンスを活用しています。自社が属する業界に対し、「どのような攻撃グループが」「どのような攻撃手法を用いて」「どのような攻撃キャンペーン（作戦活動）を展開するのか」を分析しながら、ダイナミックなセキュリティ対策を考えて、最も費用対効果の高い対策を導出しているのです。

組織のCyber IQを高めるためには、サイバーインテリジェンスの活用とセキュリティ管理体制をタイムリーに照合することが求められます。そのアプローチは以下のとおりです。

ステップ1 サイバーインテリジェンスの構造化

サイバーインテリジェンスは一連のナラティブ（narrative＝物語）な文書で識別されることが多いといえます。その場合、定性的な文章で記されたインテリジェンスをそのまま活用することは非常に困難です。そのため最初のステップは、「攻撃アクター」「対処する業界」「そこで使われるテクニック」というように、文書を要素分解して構造化します。

ステップ2 セキュリティ管理体制と評価

ステップ1で構造化した攻撃手法を、「最新の攻撃シナリオ」と「自社のセキュリティ体制」のマトリクス形式にまとめて整理します。これにより、新たな攻撃手法に対して最適な防御対策が講じられているのかを可視化できます。

ステップ3 導出された対策の実行

ステップ2で整理した表をもとに、セキュリティ対策が網羅されていない領域を洗い出し、その対策を立案します。なお、その際にはリスクの大きさに対する投資有効性の観点からリソースを配分し、ROI（費用対効果）の高い対策から優先して適用していきます。

［図表13］ インテリジェンスを活用したダイナミックなセキュリティへの転換

1 サイバーインテリジェンスの分析

サイバーインテリジェンスを構造化し、攻撃シナリオを分析

背景動向	APT-XXは、アジア諸国を対象とした…	Medium	構造化	APT-XX / Mobile OS / SMS / 情報窃取
示唆	これらの脆弱性が利用されていることから…	Important		
背景動向	PwCは、キーロガーによって窃取された…	Medium	構造化	Red Dev 18 / Software XX / Malware / キーロガー
示唆	古い攻撃手法であるが、被害が広く確認されており…	Important		

2 自社のセキュリティ管理体制評価

「最新の攻撃シナリオ」と「自社のセキュリティ体制」をタイムリーに照合

攻撃シナリオ	自社のセキュリティ体制：事務LAN / PC端末 パッチ適用	多要素認証	NW IOC適用
攻撃手法A	未	N/A	済
攻撃手法B	済	N/A	一部未
攻撃手法C	済	一部未	済
攻撃手法D	済	N/A	済
NEW 攻撃手法E	未	未	未

3 導出された対策

費用対効果の高い対策を導出

	パッチ適用	多要素認証	IOC適用
効果	High	Middle	Middle
緊急性	Urgent	Low	Middle
リソース	中	大	小
	即時対応	計画的に対応	即時対応

対リスクROI（リスクの大きさに対する投資有効性）の観点で、リソースを配分

ただしこのアプローチは、現場の技術的な話が中心となり、機関投資などのステークホルダーには説明が難しいという課題があります。

そのため次のステップでは、対策の内容とその有効性を、セキュリティの専門知識がない相手が理解できるようにするといった作業が必要です。つまり、**サイバーインテリジェンスから導出された指標を、経営層が“腹落ち”する形で可視化する**のです。

CEO（最高経営責任者）やCOO（最高執行責任者）に対してサイバー脅威の技術的な手法を詳説することは賢明ではありません。彼らが知るべきは、サイバー脅威がビジネスの継続性や自社の信用、知的財産に対してどのくらいダメージを与えるかです。「自社のサイバーリスクは何か」「現状、そのリスクが低減できているのか」「残余しているリスクは何か」「その残余リスクに対して追加アプローチを取る必要があるのか」といった自社のサイバーリスク状況を適切に把握し、情勢判断と意思決定を下せるような環境を構築しなければなりません。

そのためには、インテリジェンスから導出された指標を使用しながらBI（Business Intelligence）ツールでダッシュボードを作成し、意思決定に役立ててもらいます。「ダッシュボードを見ながら経営者が意思決定をする」という仕組みは、これまでも数多くの経営者が行っているので、抵抗はないでしょう。

おわりに

「最後は人」と言われるサイバーセキュリティにおいて、経営層を含めた人材・組織が自組織のビジネスゴールを共有しながらも共通のリスク認識を持ち対処すること、そのための仕組みを構築して運用することは、およそ一筋縄ではいかない経営課題といえます。

この課題を解くためには、本編でも述べたとおりサイバーインテリジェンス、およびその活動を推進、実行する人材が必要不可欠です。こうした人材の採用・育成とそれを実践するビジネスの現場は不可分の関係にあります。そのためこれまで以上にサイバー人材に対する魅力付けや外部へのアピールを行うことが重要となるでしょう。

組織のサイバーセキュリティの在り方を進化させることが企業の成長戦略においても重要な時代となっています。

お問い合わせ先

PwC Japanグループ
www.pwc.com/jp/ja/contact.html

監修

林　和洋
PwCコンサルティング合同会社
サイバーセキュリティ&
プライバシー リーダー
上席執行役員　パートナー

丸山 満彦
PwCコンサルティング合同会社
パートナー

執筆

村上 純一
PwCコンサルティング合同会社
ディレクター

上杉 謙二
PwCコンサルティング合同会社
ディレクター

長山 哲也
PwCコンサルティング合同会社
マネージャー

澤山 高士
PwCコンサルティング合同会社
シニアアソシエイト

www.pwc.com/jp

発刊年月：2023年1月　　管理番号：I202208-09