PwC's Cyber Security Insights 2021

ニューノーマルやDXがもたらした新たなサイバーセキュリティ

pwc

www.pwc.com/jp

はじめに

新型コロナウイルス感染症（COVID-19）や世界情勢などの影響によりビジネス環境が大きく変化し続ける中、企業はAIやIoT、ビッグデータ、5Gといったデジタルテクノロジーを活用し、競争優位性を中長期的に確立するビジネス変革が求められています。

企業がデジタルトランスフォーメーションを推進し、かつ高度なサイバー攻撃に対峙するためには、クラウドの活用といったITの技術的な対応に加えて、ビジネスにおけるユースケースの進化・高度化が必要となります。

デジタルビジネスにおいてシステムの安全性を確実に担保するために何をするべきか。従来のセキュリティとの考え方の違いや対応すべき事項について以下を重要と考え、企業の適用に向けての論点を解説します。

ゼロトラスト・アーキテクチャ

ゼロトラスト・アーキテクチャは利便性やセキュリティの向上させることには間違いありませんが、特有の考慮事項やハードルが存在します。ゼロトラストの概念を用いてセキュリティを推進するための課題や成功に向けたアプローチを「次世代のITインフラ - ゼロトラスト・アーキテクチャ」といった内容で取りまとめました。

デジタルビジネス開発におけるセキュリティ

ビジネスのスピードが加速し、ITにもスピードアップが求められています。変化していく状況で適切なセキュリティを確保するために、セキュリティ担当者やIT開発者が自らの役割を認識し、これまでと異なるアプローチを取る必要があります。「DXにおけるサイバーセキュリティ」として取りまとめ、新たな方法論「リーンセキュリティ」「アジャイル開発におけるセキュリティ」を解説しています。

CSIRTの高度化

従来のサイバー攻撃対策は、それを迂回する攻撃手法が台頭すると無力に等しくなるという弱点を抱えており、防御側は新しい攻撃手法に一つずつ対処していくほかないのが実情です。サイバー攻撃の驚異的な進化に対し、防御する側は後手に回っていると言わざるを得ません。サイバー攻撃に対峙するCSIRTが新たに打つべき有効施策を提言します。「CSIRTを進化させる次の一手」といった内容で取りまとめました。

Agenda

1 次世代のITインフラ ——ゼロトラスト・アーキテクチャ

1. ITインフラの役割変化とゼロトラストの適合性

1. IT利活用の変化に、インフラは追随できているか

デジタルトランスフォーメーション（DX）の必要性が叫ばれて久しい昨今、ITの技術的な側面だけでなく、ビジネスにおけるユースケースの進化・高度化が続いている。もはや「ITはIT部門が担当するもの」という考え方も薄れつつあり、「Shadow IT（IT統括部門の把握・管理外におけるデバイスやクラウドサービスの利用）」の問題顕在化が示すように、ビジネス部門も自由闊達にITを利用するようになった。

一方でITインフラは、このような変化に追随しているのであろうか。実態として、多くの企業ではEoL（End of Life）対応のリプレイスやセキュリティ機能の追加などは行っているものの、「ITインフラアーキテクチャの見直し」を行っているケースは少ないのではないだろうか。

昨今特に注目を浴びている「ゼロトラスト・アーキテクチャ」の考え方に基づくITインフラアーキテクチャの見直しを見据え、次の2点について触れ、自社のITインフラをゼロトラスト化する意義を中心に解説していく。

- 今日におけるITやそのユースケースがもたらす、ITインフラへの要求変化
- ITインフラへの要求に対するゼロトラスト・アーキテクチャの適合性

2. ITインフラへの要求に変化をもたらす要素

ITインフラに要求されることを考えるために、まずは企業を取り巻く状況を見ていこう。

・ビジネスのデジタル化およびアジリティ向上

今やDXを意識しない企業はないと言ってよいほど、デジタル化の波はビジネスに大きな影響を及ぼしている。DXは、単にビジネスにITを組み込むことに留まらない。業種・業態の境界線を越えてスピーディーにビジネスを展開するために、ビジネスとITを密に組み合わせ、アジャイルにシステムを構築する動きにつながっている。これにより、社内のIT部門のみならずビジネス部門、さらには社外の関係者がタッグを組むなど、1つのIT環境の中に多様な人物が入り混じる構図が生まれている。

また、上記と関連したクラウドサービスの利用拡大も無視できない。クラウドサービスは、IT利活用ひいてはビジネス自体のアジリティ向上に寄与するが、一方でコンプライアンスとセキュリティにおけるリスクを浮き彫りにもしている。

・働き方改革・リモートワーク定着の潮流

新型コロナウイルス感染症により、多くの企業では在宅勤務（リモートワーク）へのシフトが行われた。では、この「リモート化」の潮流は、いわば一過性のBCP（Business Continuity Plan：事業継続計画）対応として、事の収束と共に縮小していくのだろうか。私たちはまた、これまでと同じようにオフィスに出社して仕事をするようになるのではないだろうか。

今回の潮流によって、「出社しなくても十分に仕事ができる」と気付く従業員が一定数いるものと考えられるし、従来から子育て・介護などを筆頭に「出社しないワークスタイルが望ましい」層もいる。リモートワーク制度の整備・浸透度合いが、人材獲得ひいては競争力の源泉となるシナリオも十分現実的である。

・サイバー攻撃の巧妙化

多くの企業は、エンドポイントセキュリティおよびネットワークセキュリティを筆頭に、種々のセキュリティ対策を打っている。一方、そのような企業であっても、残念ながら被害に遭ってしまうケースが後を絶たない。

認証された端末が侵害を受け、それがネットワークを通じて他のシステムに波及する、もしくは認証されたユーザーが意図的な不正を働くケースなど、セキュリティ対策でカバーし切れない「抜け穴」を突かれるケースも枚挙にいとまがない。

上記の要素を勘案すると、ITインフラには「インフラたる安定性や安全性」を維持しつつ、より高度な認証・認可の機能、ならびにビジネスに対応するアジリティが要求されていると言える（図表1）。

3. ITインフラへの要求に応えるゼロトラスト・アーキテクチャ

こうした複雑かつ広範な対応を求められる現代において、注目されるセキュリティの概念がゼロトラスト・アーキテクチャである。ゼロトラスト・アーキテクチャは、その名の通り「信頼しない」こと、つまり「毎回認証・検証すること」を基本的な考え方としている。端末の接続ネットワークが社内LANであろうとインターネットであろうと、手放しで信頼することはない。裏を返せば、社内LANに接続されていないユーザーやデバイス（社外の関係者やリモートワーカー）であっても、同様の安全性を担保することが可能になるわけである。これは、接続元ネットワークを問わず、統合的にユーザーやデバイスおよびコンテキストに基づき認証・認可を行うことで実現される（図表2）。

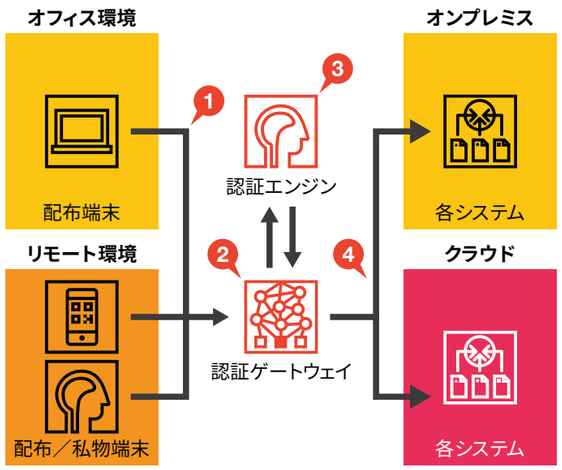
この考え方は、上述したITインフラへの要求の変化にも合致する内容である。ゼロトラスト化により、安定的・安全かつ柔軟なITインフラを実現可能である（図表3）。

ここまで読む限り、「ゼロトラスト・アーキテクチャはよいことづくしである」と思われるかもしれない。では、全ての企業は、すぐにゼロトラスト・アーキテクチャの導入に着手すべきなのだろうか。

図表1：企業を取り巻く状況とITインフラへの要求

	何が起きているか？	ITインフラへの要求は？
ビジネスのデジタル化・アジリティ向上	・システム利用者・アクセス者の多様化（社内外を問わない）	社外であってもセキュアに、最小権限で個別のシステムにアクセスできること
	・システム利用開始までのリードタイム短縮（個別のセキュリティ対策検討が間に合わない）	公開システムを除き、システムを直接触りに行けないこと
働き方改革・リモートワーク定着	・システムに対する、外部を送信元としたアクセスユーザーおよびトラフィックの増加 ・リモート環境整備・効率化の必要性（業務効率化とセキュリティの両立）	VPNに依存しないシステムへの接続および認証・認可
サイバー攻撃の巧妙化	・1つの端末を起点とした侵害の横拡大（ラテラル・ムーブメント）	ネットワークへの参加を信頼の条件にしない
	・正当な権限を持つユーザーによる侵害（内部犯行）	デバイスの状態やユーザーアクティビティのチェック

図表2：ゼロトラスト・アーキテクチャの概要



1. 社内／外などのアクセス元を問わず原則全ての通信経路は同じ
2. 認証・認可のために、IdPなどへアクセスを集約VPNのようにTrustネットワークへアクセスさせる手法は取らない
3. ユーザー・デバイスおよびコンテキストで、認証・認可を判断
4. オンプレミス／クラウド問わず、システム側でのローカル認証は原則行わない

図表3：ゼロトラスト・アーキテクチャの特徴

ITインフラへの要求は？	要求に対するゼロトラスト・アーキテクチャの回答	
社外であってもセキュアに、最小権限で個別のシステムにアクセスできること	一元的な認証	・システムに直接アクセス・認証しに行くのではなく、IdP を経由 ・VPN を使わなくとも、インターネットからシステムにアクセス可能 ・LAN に接続する必要がないため、社外のユーザーもアクセス可能
公開システムを除き、システムを直接触りに行けないこと		
VPNに依存しないシステムへの接続および認証・認可		
ネットワークへの参加を信頼の条件にしない	ネットワークによる認証の撤廃	・自社のデータセンターを経由せず、直接クラウドにアクセス→ローカルブレイクアウトなど、ネットワーク側の考慮不要 ・送信元 IP アドレスや所属ネットワークではなく、デバイス・ユーザーおよびコンテキストで認証
デバイスの状態やユーザーアクティビティのチェック		

2. ゼロトラストへの移行に際する検討・留意事項

1. 自社はゼロトラスト化すべきなのか？できるのか？

ゼロトラスト・アーキテクチャは、一見すると企業のセキュリティ上の諸課題を解決する打ち手に思われる。それは間違いではないが、一方で、安易に「我が社もゼロトラスト化を」と進めてしまうと、思わぬ落とし穴にはまってしまう可能性がある。

ゼロトラスト・アーキテクチャは現代のITユースケースに適合するからこそ注目を浴びている考え方だが、現状ではいわば「バズワード」の域を出ない。また、利便性やセキュリティを向上させることは間違いないが、ビジネスを営む上で「ゼロトラスト・アーキテクチャでなければ成り立たない」わけでもない。そのため、まずは「なぜ自社にゼロトラスト・アーキテクチャが必要なのか」を明確にする必要がある。そうでないと、そもそもの必要性、もしくは変革にかかるコストおよび人的負荷など、ステークホルダーからの疑問に答えることができない。

また、「アーキテクチャ」という単語が入ることからも、ゼロトラスト・アーキテクチャへの変革は、ITインフラのアーキテクチャ変更を意味する。それには特有の考慮事項やハードルがあるので、これを踏まえなければ思わぬところで足元をすくわれたり、結果としていびつなアーキテクチャが出来上がったり、という結末を招く危険性がある。

これらの視点を踏まえ、企業がゼロトラスト化を推し進める際の要諦について触れていく。

2. アーキテクチャを変えるということ

ゼロトラスト・アーキテクチャは概念であるため、特定の機能を持つソリューションや製品を指すものではない。既存の構成に何かを組み込んで終わりというものではなく、「どうやってゼロトラスト・アーキテクチャを実現するか」という、自社なりの解釈が必要である。また、ゼロトラスト・アーキテクチャは目的ではなく手段なので、まずは自社におけるITのユースケースや働き方などに関する未来像を描き、その実現手段としてゼロトラスト・アーキテクチャが適切であるかを吟味する必要がある。その後で、自社の現有資産などを考慮しつつ、それを実現するためのソリューション・製品を選定していくべきである（図表4）。

また、前述のように、ゼロトラスト・アーキテクチャへの変革はアーキテクチャの変更を伴うものである。つまり、多くの企業にとってITインフラの「抜本的な変革」になり、ゆえに多額の予算を要する場合があるし、各システムの管理部門に協力を依頼するべき箇所もある。ワークスタイルやシステムのユースケースに関するデザインと密接に関連することからも、IT部門だけでなく、多くの関係者を巻き込みながら推進すべきである。

図表4：アーキテクチャの変更に際して検討していくべきこと

1 ありたい姿	2 あるべき姿	3 実現可能な姿
・実現したい「働き方」 －働く場所 －利用するデバイス －社外関係者との情報授受やコラボレーション －コミュニケーションの方法 ・上記を実現するための「ITの使わせ方」	・ビジネス特性やミッションに鑑みた、ふさわしい働き方や情報の取り扱い方法 －業界慣習や規制 －取り扱う情報の性質（機密性） －ステークホルダーの要望・期待	・現在の姿から逆算したフィージブルな着地点 ・現有するシステムやセキュリティ対策との互換性、ならびに予定している更改時期 ・コスト的な制約 ・グローバルやグループ会社に対するガバナンスの関与深度

3. ゼロトラスト・アーキテクチャへの変革に向けた考慮事項

ここからは、企業がゼロトラスト・アーキテクチャを導入する上で考慮すべき事項を見ていこう。

(1) どこから、どのようにしてゼロトラスト化していくか

ゼロトラスト・アーキテクチャへの移行は、企業のサービスや製品のユーザーの通信フローに変化を及ぼすことから、少なからずユーザーエクスペリエンスに影響を与える恐れがある。そのため、全システムを対象として一斉に移行することは、ユーザーサポートなどの現実的なオペレーションを考慮して「ほぼ不可能」と考えるべきである。詳しくは後述するが、「どのシステムまたはユーザーを」、「いつ・どのような順序で移行していくか」といった視点で移行計画を立てることが重要である。

また、中長期でクラウドマイグレーションを行い、それを終えたシステムから順次ゼロトラスト環境に組み込んでいく、もしくはそもそも「全てをゼロトラスト化しない」という考え方もあり得る。このような場合においても、移行計画が重要なことは言うまでもないが、「ゼロトラストな環境」と「従来型（ペリメター）環境」が併存することによるコストや運用負荷を最小化するための考慮が併せて必要となる。

(2) ソリューション・製品の導入に伴い必要な実施事項はないか

前述のように、ゼロトラスト・アーキテクチャを実現する上では、自社に最適な製品・ソリューションの組み合わせを検討する必要がある。その際、主に認証に関して、ソリューション導入と並行もしくはそれに先行して、自社内で実施すべきタスクが想定される。そのため、これらにかかるリードタイムをあらかじめスケジュールに組み込んでおく必要がある（図表5）。

(3) グループ会社や海外拠点をどう扱うか

ゼロトラスト化にあたっては、グループ会社や海外拠点をどこまで巻き込むのかも考える必要がある。グループ内におけるITシステムの共通化が進んでいるのであれば、当然グループ全体がゼロトラスト化の対象になるだろう。そうでない場合でも、海外拠点を含めて、グループ内におけるITガバナンスおよびセキュリティガバナンス強化を目指している企業も多いと思われる。ゼロトラスト・アーキテクチャでなくても、アーキテクチャの抜本変革はグループ全体のガバナンス変革のレバーになり得る。

また、ゼロトラスト化を契機としてグループ内および各国のソリューションを統合し、IT調達の最適化を図るという手もある。いずれにしても、「どこまで深くテコ入れを行うか」について検討しておくべきである。

次に、ゼロトラスト・アーキテクチャへの変革に向けた考慮事項をまとめる（図表6）。ゼロトラスト化はITシステムを変えるのみならず、自社のセキュリティやITの使い方・働き方をも変革し得るものであり一朝一夕に導入できるものでもない。しかしながら、第1回で述べた通り、ゼロトラスト化は近年のITインフラへの要求の変化に合致するものであり、安全かつ柔軟なITインフラの実現を可能にするものと筆者は考える。社内外のステークホルダーと連携・協議し、メリット・デメリットを吟味した上で変革を進めていただくことを切に願う。

図表5：ソリューション・製品の導入にあたり考慮すべきことの例（認証観点）

デバイス	・どのデバイス（配布／私物やPC ／スマートデバイスなど）で、どのシステムにアクセスさせるか？ ・上記デバイスをどのように管理するか？ ・アクセス時、どのようにしてデバイスの正当性を判別するか？ ・デバイス使用の申請から承認までを、どのように行うか？
ユーザー	・認証の根源とするユーザー・グループなどを、どこで管理するか？ ・社外のユーザーをどのように扱うか？ ・定めたルールを逸脱するケースが発生した場合、どのようにしてその承認を行うか？
コンテキスト	・上記以外に、どのような情報を利用して認証・認可を行うか？ ・不正なアクティビティやサイバー攻撃の兆候をどのように監視し、不正や侵害が検出された場合にどのような処置を行うか？

図表6：ゼロトラスト・アーキテクチャへの変革に向けた考慮事項

視点	考慮事項の例
1 どこから、どのようにしてゼロトラスト化するか？	・パイロット対象は？その後はどのような順序で移行していく？ ・移行の方法や期間中のサポート体制は？ ・そもそも全てをゼロトラスト化するのか？ ・ゼロトラストとそうでない環境を、コストや運用効率を考慮してどう併存させるのか？
2 ソリューション・製品の導入に伴い必要な実施事項はないか？	・どのようなデバイスに対して、どのような権限を割り当てるか？そのデバイスをどのように認証するか？ ・どのようなユーザー、グループおよびサイトなどに対して、どのような権限を割り当てるか？ ・どのようなコンテキストで認証するか？
3 グループ会社や海外拠点をどう扱うか？	・グループ会社や海外拠点を含めて、ゼロトラスト化の対象とするか？ ・その際、製品の統一や調達の最適化を行うか？ ・これを機に、IT ／セキュリティガバナンスの強化を行うか？

3. ネットワーク視点で捉えるゼロトラストの必要性

1. ネットワーク視点で捉えるゼロトラスト

社内のネットワーク構築においては、これまでデータセンターを中心に設計をしてきた企業や組織が多いのではないだろうか。しかし近年、クラウドサービスの利用が急激に進み、これからはクラウド環境を中心にした設計にシフトする必要が出てきている。

こうした環境下、企業のIT担当者はクラウド向けのトラフィックのマネジメントに苦慮してきたことかと思われる。これに加えて、新型コロナウイルス感染症をきっかけにする在宅勤務（リモートワーク）の増加で社外から自社のデータセンターやクラウドサービスへ接続するといった、管理するべきトラフィックの経路が増えてきている。企業においては、従来のデータセンター中心のトラフィックマネジメントのやり方を再考する時期に来ているのではないかと考えている。近年顕著になっている企業ネットワークの課題とリモートワーク推進により新たに生じた課題をピックアップし、ゼロトラスト化の必要性について、ネットワークの観点で解説する。

2. クラウド利用の急増が与えた企業ネットワークへの影響

データセンター上で稼働していた業務アプリケーションをクラウド上のサービスに切り替える動きが増えている。一方でクラウド利用に伴い、いくつかの問題が生じている企業が出てきている。例えば、通信トラフィックが多く発生するコラボレーション系のソフトウェアをクラウドに移行することで、データセンターとクラウドサービスをつなぐ回線が混雑し、利用者のユーザビリティを著しく低下させるという問題が発生している。

またデータセンター内のサーバー環境、ネットワーク環境を仮想化しクラウドのIaaS（Infrastructure as a Service）基盤とシームレスに連携するハイブリッドな環境の構築も進んできている。クラウド環境向けネットワークに対して求められる可用性やパフォーマンスは、ますます高くなってきている。

この問題を解消するために、多くの企業は回線帯域の増強を行ってきたのではないだろうか。この対策はセキュリティのガバナンスを維持しつつ至急打てる策の一つではあるが、長い目で見た時に、データセンター内の他のリソース（通信機器、プロキシサーバーなど）も消費し、各拠点をつなぐアクセス回線の帯域も圧迫させるため、恒久的な策とは言えない。

3. リモートワークがもたらした新たな課題 ――境界型アーキテクチャの限界

新型コロナウイルス感染症をきっかけに、リモート環境でPCを利用するのが当たり前になった。リモート環境でPCを利用するにはこれまで、業務上必要な場合、社内の申請手続きを経る必要があった。そのため、利用されるPCの台数は多くなかった。しかし、リモートワークが推奨されるようになり、社内で利用されるPC台数よりリモート環境で使われるPCのほうが多くなった。社員のほとんどがリモート環境でPCを利用する場合、ネットワークに求められる新たな要件を考察すると、大きく以下の2つが言えるかと思われる。

（1）セキュアにクラウド環境にアクセスできること

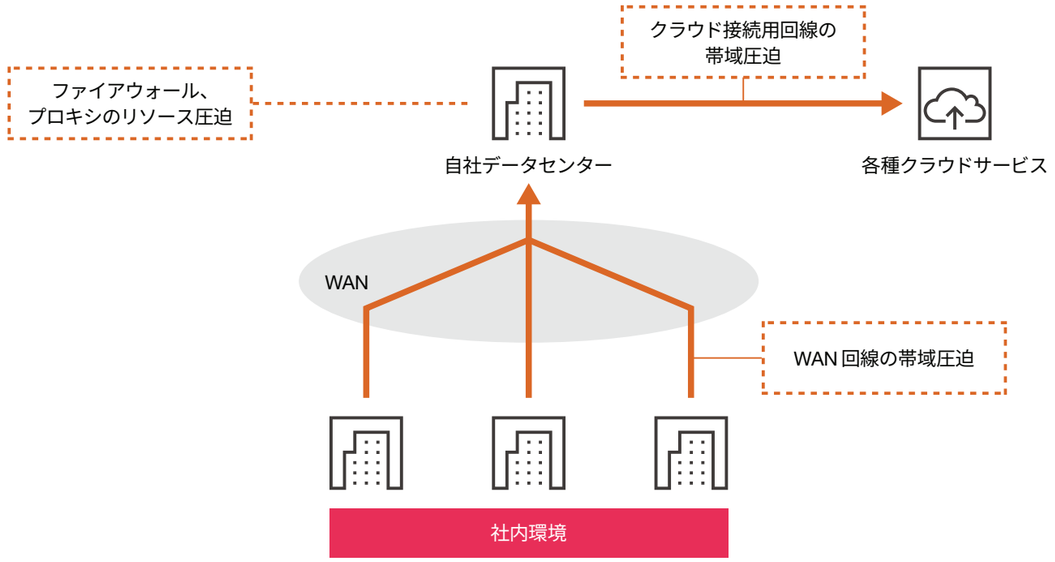
これまでのようなオンプレミスの境界型のセキュリティ装置で担保されていた仕組みが効かない、オープンなインターネットの領域からクラウド環境にアクセスすることになるため、ウイルス感染やデータ漏えいへの対策をネットワーク上の新たな仕組みで補う必要が出ている。

（2）社内システムに一斉にアクセスしても耐えられるキャパシティを用意すること

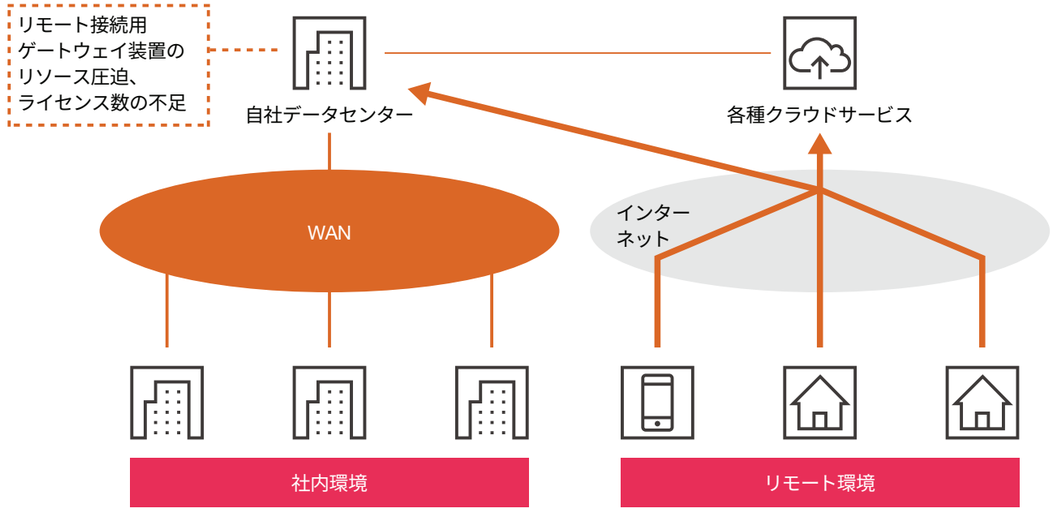
これまでは、業務で必要となる社員が申請してPCを利用するといった対応をしていたため、接続台数はある程度予測でき、急激に変化するということはなかった。しかし、社員の多くがリモートワークに切り替わることにより、これまでの想定より多くのPCがリモートアクセス用のゲートウェイ装置などに接続してくるという状態になっていた。これにより多くの企業は、装置の処理性能や接続用のライセンスが不足するといった状況に陥った。

この2つの要件を、境界型のアーキテクチャで数日から長くて数週間で対応することは、極めて困難である。企業のIT担当者にとっては、境界型のアーキテクチャの限界を肌で感じる象徴的な出来事だったのではないだろうか。

図表7：クラウド利用の急増による通信のボトルネック



図表8：リモート環境の利用増による通信のボトルネック



4. 今後、どうするべきか
――変革を実現する重要な論点

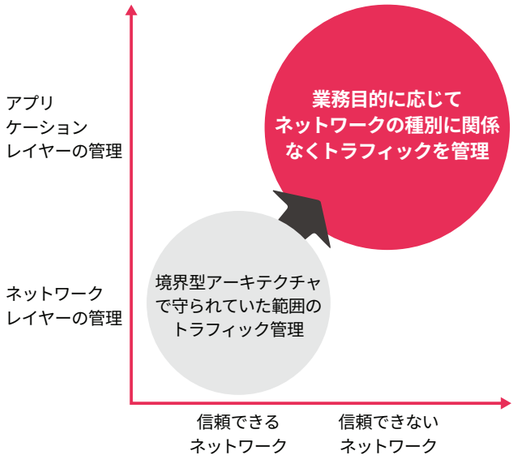
これからのネットワークに求められる要件に応えるためには、従来の境界型で守られていた範囲を管理するという考え方から、社員の働き方を中心に捉えて、業務の目的に応じてネットワークの種別に関係なくトラフィックを管理する、という考え方に変える必要がある。そのためには、これまで閉域網におけるIPベースでの管理から、業務内容により近いアプリケーションレベルでトラフィックを管理していくこと、さらにリモート環境でPC利用することを前提としたセキュリティリスクなどを管理していく必要が出てくる。

アプリケーションレベルでトラフィック管理を行うには、SDN（Software Defined Network）の技術が必要になって来る。IPベースで設計された物理的なネットワーク（アンダーレイネットワーク）による制約を受けずにコントロールできるため、オーバーレイネットワークとも呼ばれる。SDNの技術を用いたWAN（Wide Area Network）のソリューションが、SD-WANである。アプリケーションを識別する機能を持ったSD-WANルータでクラウドサービス向けのトラフィックを集中的にコントロールすることができ、企業のネットワークを支える技術の大きな柱になってくる。

次に、インターネットのような必ずしも信頼できないネットワークを利用する場合のリスクを管理するために必要となってくるのが、ゼロトラスト・アーキテクチャの概念である。全てのトラフィックを信頼しないことを前提に検証することで、ネットワークを脅威から守るというアプローチである。デバイス、ユーザー、アプリケーション、トラフィックそれぞれの視点でリスクが存在しないか検証を行い、安全との確認が取れたもののみ利用を許可する。ゼロトラスト・アーキテクチャは概念であるため、自社の要件をもとに、どの製品ベンダーのソリューションが最適なのか、評価を行った上で導入を進めていく必要がある。自社に最適なゼロトラストのソリューションを採用することで、安全にリモートワークができるようになる。

今後、ビジネス環境はさらに急激に変化していくことが想定される。企業はそれに対応するために、ゼロトラストなネットワークになるための準備を今から進めていく必要がある。

図表9：今後のトラフィック管理の方向性



4. ゼロトラストの実現に必要な機能および構成の例

1. ゼロトラストは、どのようなソリューションで実現するのか？

これまでに記載した通り、ゼロトラスト･アーキテクチャは概念であり、特定のソリューションを指すものではない。とはいえ、それを実現する立場であるクライアントからは、「結局、何を使ってどう実現すればよいのか」といった旨のお問い合わせをいただくことがある。

実際には、各ベンダーがそれぞれのシーズでゼロトラストを解釈していることから、製品／ベンダーによって多様な実現方法があるのが実態である。そのため、ソリューションへ紐づけることが困難な側面があるのだが､ここでは｢ゼロトラスト･アーキテクチャの実現に求められる機能」を考え、それを実現するための一般的なソリューション例を紹介していく。

2. ゼロトラスト・アーキテクチャの実現に求められる機能

P4「ITインフラの役割変化とゼロトラストの適合性」で述べた通り、ゼロトラスト・アーキテクチャでは、ユーザーやデバイスおよびコンテキストに基づき正当性・信頼性を検証し、その結果に基づきシステムやデータなどへのアクセス可否を判断するという考え方を採用する。そのためには、例えば以下のような機能を具備している必要がある。

ユーザーの正当性・信頼性の検証

- そもそも正しいユーザーなのか（本来アクセスを許可されているのか）を検証していく。これは、ゼロトラストでなくとも既にほとんどのシステムで実装されているが、ゼロトラスト・アーキテクチャにおいては、IdP（Identity Provider）に一元的なユーザーの認証の仕組みを付与し、その背後でディレクトリサービスに問い合わせを行うような場合が多い。
- アクセス者が正しいユーザーであったとして、場合によっては「本当にそのユーザーが意図してアクセスしたものなのか」を検証する必要が生じるだろう。つまり､正しいユーザーが侵害されたことによる不正アクセスではないかを確認する。これはトークンや生体などを用いた、2要素目以降の認証によって実現されるものである。この認証も、上記同様にIdPで実現するケースが多数を占める。

デバイスの正当性・信頼性の検証

- ユーザーと同様、データやシステムにアクセスすることが許可されているデバイスであるかを検証する。クライアント証明書によって認証するケースが多いだろう。ただし、一概に許可／拒否を判断するだけでなく、仮にクライアント証明書がない場合（私物デバイスなど）でも、特定の行動（読み取り専用など）であれば許可する、などの制御を行う場合もある。これは、ユーザーと同様にIdPで認証を行い、背後のデバイス管理ソリューション（MDM：Mobile Device Management, EMM: Enterprise Mobility Management, またはUEM：Unified Endpoint Managementなど）に問い合わせることで実現できる。
- 許可されたデバイスだとして、それが「アクセス許可に足る状態なのか」を検証する。つまり、パッチやパターンファイルが適用されていない、あるいはOSのバージョンが最新ではないなど、許可しているデバイスであっても望ましくない（リスクがある）状態の場合､アクセスさせない､といった判断がなされるべきである。これも上記同様のデバイス管理ソリューションで実現できる。

コンテキストの検証

- ユーザーやデバイスが認証された状態であったとしても、その行動が適切であるかを検証する必要がある。例えば、社内の機密情報を、許可していないクラウドストレージへアップロードするような動作があった場合、それは遮断または検知されるべきであるし、許可しているクラウドもしくはオンプレミスであっても、不審または不正な行動は検知され、アクセス権を剥奪するなどの対応が求められる。この実現にはさまざまな方法が考えられるが、代表的なものを以下に記載する。
  - CASB（Cloud Access Security Broker）を用いて、許可していないクラウドサービス（Shadow IT）の利用を検知・制御、ならびに許可したクラウドサービスにおける行動（データのアップロード、ダウンロードまたはコピー・編集など）を制御
  - RM／DRM（Information／Data Rights Management）またはDLP（Data Loss Prevention）製品などを用いて、

データの持ち出し検知・制御、または有事におけるトレーサビリティを確保

- SIEM（Security Incident and Event Management）またはUEBA（User and Entity Behavior Analysis）で上記ソリューションやデバイスのログを分析の上、不審な兆候を検知し、その結果に基づき不審なユーザーや端末を遮断

・ユーザーやデバイスが認証された状態であったとしても、その後に侵害を受ける（マルウェア感染など）可能性もある。そのため、継続的に状況を監視の上、必要に応じて遮断する必要がある。これにはEPP（Endpoint Protection Platform、アンチウイルスソフト）やEDR（Endpoint Detection and Response）を用いる。また、インターネットアクセスの状況を監視・制御するという意味でSWG（Secure Web Gateway、クラウド版プロキシのイメージ）の利用も有効である。

ここまでに記載した内容を簡単にまとめると、以下のようになる（図表10）。こうして一覧化してみると、ゼロトラスト・アーキテクチャは、概念としては新しいものの、その実現に用いるソリューション群自体は目新しいものばかりではないことが分かるのではないだろうか。

（任意）経路の変更

ゼロトラスト・アーキテクチャでは、特定のネットワーク（企業のLANなど）に参加していることを条件としたアクセス許可を行わない。つまり、自宅やカフェからでも、オフィスからでも、等しくデータやシステムにアクセスできる環境が必要となる。一方、アクセス先のデータやシステムは未だにオンプレミス環境内に存在する場合もあり、インターネット越しにアクセスさせることのリスクがある。

その場合は、SDN／SD-WAN（Software-Defined Network／WAN）を用いて、アクセス先のシステムに応じて経路を変更するなどの方法が採られる場合もある。ただし、リバースプロキシなどを用いて、インターネットから安全にアクセスする方法も存在する。

3. ゼロトラスト・アーキテクチャの実現の例

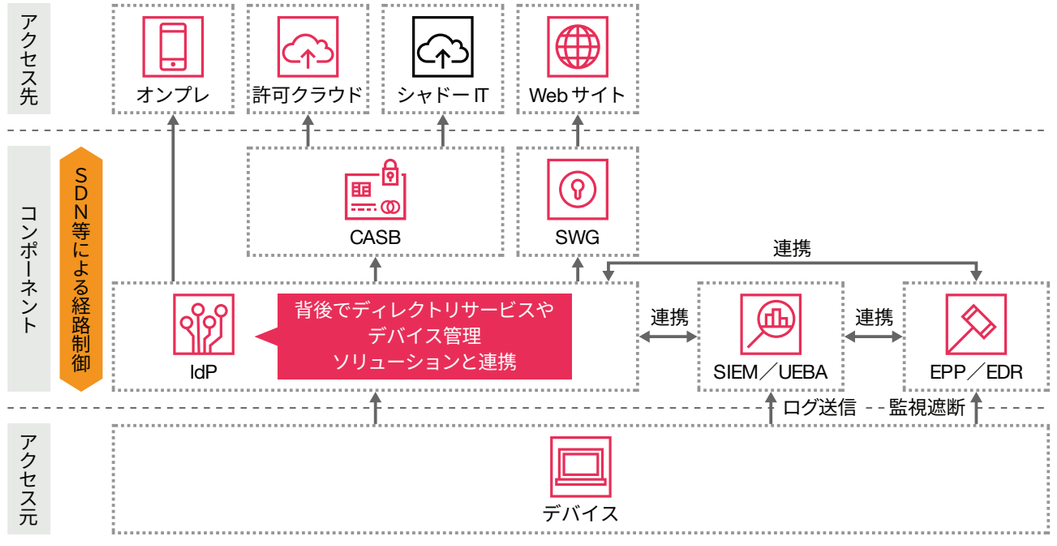
これまでの内容に基づき、ゼロトラスト・アーキテクチャを実現した場合のセキュリティアーキテクチャについて、一例を図示する（図表11）。ただし、冒頭に記載した通り、解釈によって多様な実現方法があることから、これが決して唯一の解ではないことに留意してほしい。

いずれにしても、各ソリューションの機能・コスト優位性、既存ソリューションとの互換性・親和性、もしくはグループ会社や海外本社・支社との兼ね合いを踏まえて、各企業で適切なソリューションを検討・選定していくことになる。

図表10：ゼロトラスト・アーキテクチャの実現方法の例

検証対象	検証内容の例	実現方法の一例
ユーザー	・正しいユーザーか（アクセスを許可されたユーザーか） ・アクセスの真正性（そのユーザーが意図したアクセスか）	・IdP: Identity Provider + ディレクトリサービス + MFA: Multi-Factor Authentication, ワンタイムパスワード、ハードウェアトークン、バイオメトリクス認証など）
デバイス	・正しいデバイスか（アクセスを許可されたデバイスか） ・デバイスが、アクセスを許可できる状態になっているか	・IdP: Identity Provider + デバイス管理（MDM: Mobile Device Management, EMM: Enterprise Mobility Management, UEM: Unified Endpoint Management）
コンテキスト	・行動が適切であるか（不正を働いていないか） ・侵害を受けている、またはその兆候がないか	・CASB: Cloud Access Security Broker ・IRM/DRM: Information/Data Rights Management ・SIEM: Security Incident and Event Management ・EPP: Endpoint Protection Platform ・EDR: Endpoint Detection and Response

図表11：ゼロトラスト・アーキテクチャの実現の例



2 DXにおけるサイバーセキュリティ

1. 新規事業／顧客向けサービスにおけるセキュリティ リーンセキュリティ

製品やサービスの開発手法の一つであったアジャイルは、リーンスタートアップという概念の登場により、ビジネスの世界でも活用され始めている。仮説のもとで製品・サービスを設計し、顧客に使用してもらいながら改良を重ねるリーンスタートアップの登場で、開発手法として誕生したアジャイルがビジネスのスタイルにも応用されるようになったのである。今や企業の規模に関係なく、デジタル時代の働き方・業務の進め方の手法として取り入れられている。

事業やサービスの改善を高速で回すこの手法は、事業（ビジネス）部門主導で進められる。セキュリティにおいてはこれまでのコーポレートIT、コーポレートセキュリティとは全く違った考え方が必要になってくるであろう。ビジネス部門主導で進める事業／サービスにおいて、スピードを犠牲にせずにセキュリティを担保する手法について論じていく。

1. 新規事業（デジタルビジネス）において顧客の信頼獲得を実現するには？

デジタル関連の新規事業開発の場面でよく見るのが、事業をスピーディーに進めたい事業担当者と、時間をかけて安全に事を進めたいセキュリティ担当者の間での対立である。セキュリティは本当に、スピードとのトレードオフになってしまうのであろうか。スピーディーに展開して顧客の信頼を勝ち得たいという事業サイドの事情を加味し、安全性をも担保したセキュリティを実装するにはどうしたらよいであろうか。

セキュリティの体制はこれまで、基本的には中央集権型でセキュリティ部門が独立した立場から管理するのがよいとされていた。コーポレートの基幹的な領域やベースとなるITインフラに関しては適した考え方であると筆者は思うが、これを新規ビジネスの領域に持ち込むと、管理が煩雑になってしまう。こうしたことにより、新規事業を進めるにおいてはセキュリティの考え方（求められる知識も含めて）や体制が異なってくる。

2. 新しいセキュリティの考え方の導入の必要性

デジタル関連の新規事業におけるセキュリティの導入には、どのような点を考慮することが必要だろうか。筆者は以下を重要なポイントと考える。

- 事業の特性の理解
- 事業にスピードが求められることへの最大限の理解
- 多岐にわたるステークホルダーとの調整
- 自社以外のセキュリティ対策の可能性

あらゆる分野でデジタルトランスフォーメーション（DX）が進む昨今、事業展開のスピードは格段に増し、企業や組織を取り巻くステークホルダーは広がりを見せている。同時にサイバー攻撃の手口は多様かつ巧妙になり、企業はこれまで以上に入念な対策を練る必要に迫られている。中央集権型で情報セキュリティを進めるこれまでのコーポレートセキュリティとは違う考え方を導入する必要があるであろう。

そこでPwCは、新しい時代に対応したセキュリティ対策として、「リーンセキュリティ」という考え方の導入を提言する。

3. リーンセキュリティとは？

リーンセキュリティとは、前述のようなビジネスのアジャイル化においてもスピードを落とさず、高速にセキュリティを検討していく方法論である。リーン（無駄のない）なセキュリティを実現することでビジネス部門とセキュリティ部門の対立を解消し、ビジネスに貢献できる、という考え方である。

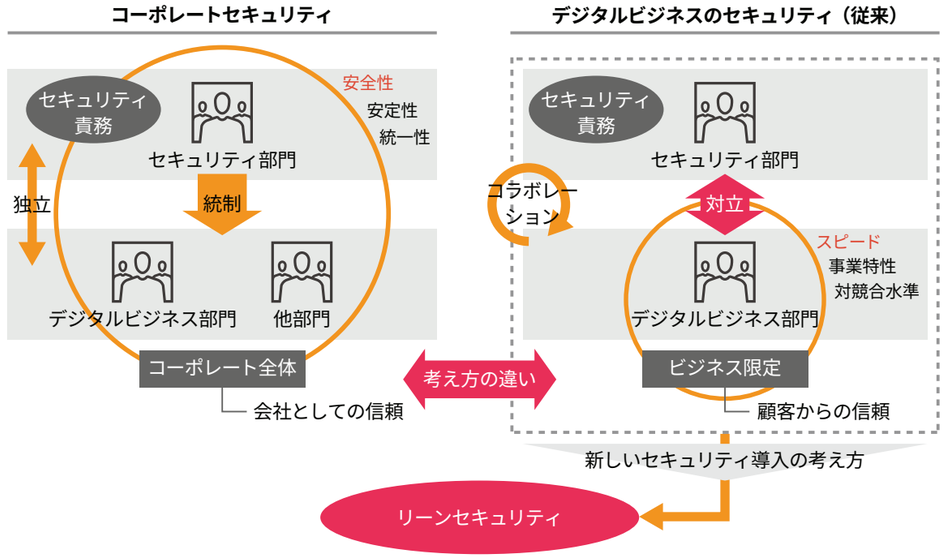
リーンセキュリティは以下の検討項目からなる。セキュリティ対策の各ステップにおいて、ポリシー、体制、プロセス、テクノロジーを対象に、あるべき姿をスピーディーに検討し、実行に移す。

どこまで中央集権型で管理するのか、どこから個別に対策を用意すべきなのか、そのバランスが重要な論点になるであろう。

図表12：これまでのコーポレートセキュリティとデジタルビジネスで求められるセキュリティの違い

新しいセキュリティ導入の考え方の必要性

・従来のセキュリティの考え方はインフラなどコーポレート全体には適しているが、
デジタルビジネスでは管理が煩雑になるため、リーンセキュリティの考えを提言したい。



図表13：リーンセキュリティにおいて各ステップで行うこと

セキュリティ対策の検討ステップ	構築ステップ	計測ステップ	学習／再配備ステップ
以下をテーマに検討する。 ・当該事業において必要になるセキュリティ態勢とは何か ・個別と共通化のバランスをどのようにとるべきか ・必要なスペックは備わっているか（個人能力も含めて）	当該事業においてセキュリティ態勢を構築する。	セキュリティの効果を測定する。	個別と共通化のバランスやリソースの再配分の検討、実行を行う。

4. リーンセキュリティを導入するには？

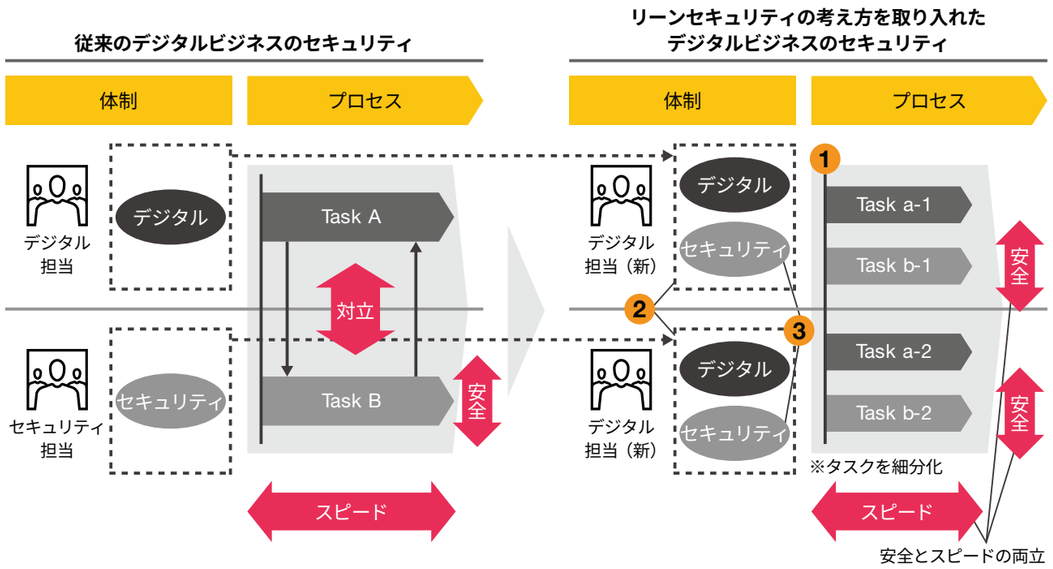
ポイントを3点説明する。

1. デジタルビジネスのサービス企画段階でのセキュリティの検討
2. デジタルビジネス担当者のデジタル＋セキュリティのスキルセット所持
3. ビジネス部門のセキュリティに関する説明責任の明確化

それぞれについて、セキュリティ対策の各ステップで検討および実施すべき内容と共に紹介する。

図表14：リーンセキュリティの考え方

・リーンセキュリティの考え方を取り入れることで担当者間の対立をなくし、スピードを落とさずセキュリティを検討できる。



リーンセキュリティの考え方	1 デジタルビジネスのサービス企画段階でのセキュリティの検討
	2 デジタルビジネス担当者はデジタル＋セキュリティのスキルセット所持
	3 ビジネス部門のセキュリティに関する説明責任の明確化

4.1. デジタルビジネスのサービス企画段階でのセキュリティの検討

デジタルビジネスの構想や予算化などのサービス企画の初期段階からセキュリティの検討を開始すべきである。これにより安全性や、信頼性、プライバシーやデータ倫理に関連するリスクを予防的に管理することができるようになる。また、同様に業務要件定義、システム要件定義段階においても、セキュリティの検討を漏れなく実施すべきである。結果としてデータセキュリティ、プライバシーなどの要件漏れによる手戻りを抑制し、セキュリティ対策の高速化を実現することができる。

検討ステップ：
- デジタルビジネス推進のプロセスとタスクを検討する。構想、予算化、業務要件定義、システム要件定義のビジネス企画段階のプロセスにセキュリティを検討するタスクが含まれているかを確認する。

構築ステップ：
- デジタルビジネス推進のプロセスとタスクを定義する。構想、予算化、業務要件定義、システム要件定義のビジネス企画段階のプロセスにセキュリティを検討するタスクが含まれていることを確認する。

計測ステップ：
- デジタルビジネスのサービス企画段階でセキュリティの検討が十分だったかを計測する。
- 計測結果を評価する。

学習／再配備ステップ：
- 検討不十分の原因を究明し、プロセスおよびタスクを見直す。

4.2. デジタルビジネス担当者のデジタル＋セキュリティのスキルセット所持

デジタルビジネスの担当者は「デジタル＋セキュリティ」のスキルセットを所持しておくべきである。デジタルビジネスでは、アイデア創出、サービス立案、概念実証（PoC）といったビジネス企画の段階でサイバーセキュリティ、データプライバシー、データ倫理に関する課題を含めた検討が必要となる。そのため、デジタルに関する知見のみならず、セキュリティのスキルセットも求められる。

デジタル＋セキュリティのスキルセットを所持することで、組織として意思統一されたポリシー／ガイドラインの下でコンプライアンスやベースラインを遵守しつつ、個人の裁量でセキュリティを検討し、関連するリスクを予防的に管理し俊敏性を損なわずにプロジェクトを推進することができるようになる。デジタルビジネスに未着手もしくは初期段階ではビジネス部門の担当者のスキルが成熟していないため、従来のセキュリティ部門からの支援や外部専門家の活用も含めて、ビジネスへの影響を極小化しつつ、段階的なスキル向上計画の推進が求められる。

検討ステップ：
- ビジネス部門が必要なセキュリティスキルセットを検討する。
- ビジネス部門は社内／社外専門家を含めセキュリティスキルセットを持つ人材の確保および配置方法の検討を行う。
- セキュリティ部門はデジタルビジネスのセキュリティ評価のための基準、プロセス、システムを検討する。
- セキュリティ部門はセキュリティスキルの評価の基準、プロセス、システムを検討する。

構築ステップ：
- 必要なスキルセットを持つ人材を配置する。
- セキュリティ部門はデジタルビジネスのセキュリティ評価のための基準、プロセス、システムを構築する。
- セキュリティ部門はセキュリティスキルの評価の基準、プロセス、システムを構築する。

計測ステップ：
- ビジネス部門はデジタルビジネスのセキュリティレベルを計測、評価する。
- セキュリティ部門はデジタルビジネスのセキュリティレベルを監査する。
- ビジネス部門は担当者のセキュリティスキルを評価する。

学習／再配備ステップ：
- ビジネス部門の担当者に不足しているセキュリティスキルセットを向上する。
- 必要なスキルセットを持つ人材をデジタルビジネスに再配置する。

4.3. ビジネス部門のセキュリティに関する説明責任の明確化

デジタルビジネスの担当者は、サイバーセキュリティ、データプライバシー、データ利用ガバナンスといった最新および今後発生するコンプライアンスなどの要求事項の説明責任の所在を明確化すべきである。セキュリティの考慮の不足を抑制し、スピード感を持ったセキュリティの検討を強制するからには、ビジネス部門はビジネスリスクと共にセキュリティリスクも負うべきであろう。例えば、ビジネス部門がセキュリティリスク対応（リスク特定、分析、対策）を実施し、セキュリティ部門はセキュリティポリシーやガイドラインを提示するといった企業組織のセキュリティ全体を統括するなど、企業ごとに適したセキュリティ領域における役割を検討し、役割に応じた責任を負うよう検討すべきである。その結果、必要に応じて組織編成の見直しや最高責任者といった役職者設置などの対応を継続的かつ柔軟に進めていくこととなる。

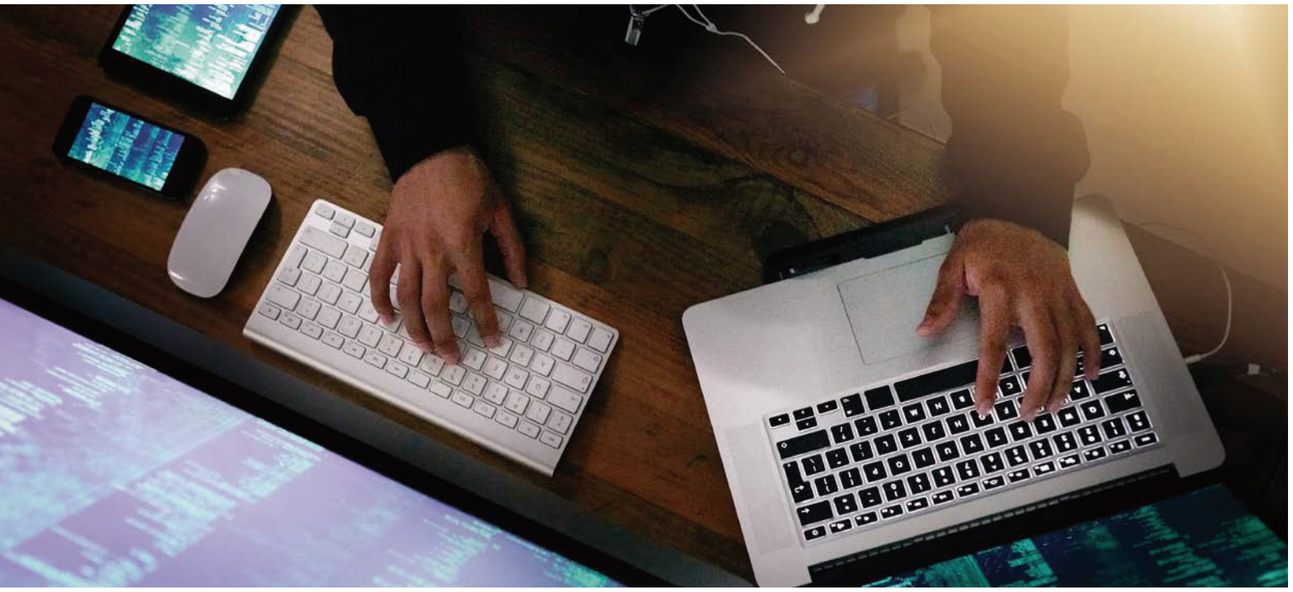
検討ステップ：
- ビジネス部門とセキュリティ部門におけるセキュリティ業務の洗い出しを実施する。
- ビジネス部門とセキュリティ部門におけるセキュリティ業務に対する役割（業務責任を負う、業務責任者支援、業務実施、業務実施支援など）の分担を定義する。

構築ステップ：
- 役割分担に応じた業務を遂行する。

計測ステップ：
- 役割分担が適切に実施できたかを計測する。

学習／再配備ステップ：
- デジタルビジネスにおけるセキュリティ業務に対する役割（業務責任を負う、業務責任者支援、業務実施、業務実施支援など）の分担を見直す。
- 見直した役割分担で業務を遂行する。

上記の3つのポイントを押さえてセキュリティ対策を実施することで、ビジネス部門主導の新しい事業やサービスにおいてもスピードを犠牲にせずにセキュリティを担保することが可能になると筆者は考える。デジタルビジネスに取り組む企業や組織においては、ぜひリーンセキュリティの考えを取り入れ、価値ある顧客体験を安全に提供できる事業／サービスの開発を推進していただければと思う。



2. アジャイル開発でのセキュリティ実装 セキュリティ担当者の役割

ビジネスのスピードが加速しシステム開発にスピードが求められるようになった昨今、アジャイル開発はスタートアップ企業だけではなく、成熟した大企業でも採用されるようになりつつある。組織の規模が大きな企業では、一般的にインフラ部門とシステム・アプリケーション開発部門は分離されており、企画・開発・運用を独自に行っているケースが多く見られる。

一方、アジャイル開発においては開発側と運用側が協力して継続的に開発を行うDevOpsが取り入れられ、部門の垣根が曖昧になりつつもある。また、コンテナ技術やサーバーレスアーキテクチャの発展により、インフラは、これまでのようにインフラ担当者に事前に用意されてアプリケーション層とは切り離されてメンテナンスされる存在ではなく、アプリケーションの一部としてデプロイされるようになっている。

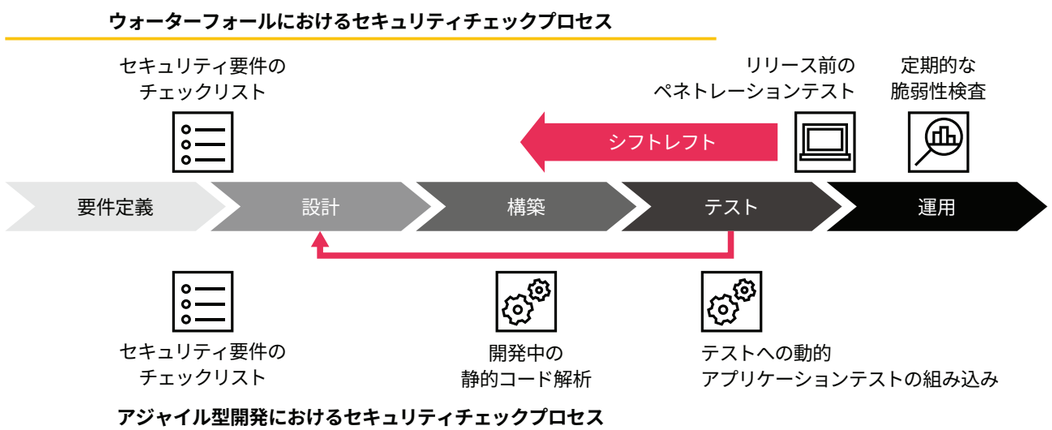
このように刻々と変化する状況で適切なセキュリティを確保するためには、アプリケーション開発者、インフラ担当者およびセキュリティ担当者のそれぞれが、変わっていく自らの役割を意識し、これまでとは異なるアプローチを取る必要がある。本章では特に大企業におけるセキュリティ担当者とインフラ担当者の役割の変化に注目することで、アジャイル開発に必要なセキュリティの実装についての留意点をまとめる。

1. アジャイル開発におけるセキュリティの確保は「シフトレフト」が鍵を握る

大企業においては、アジャイル開発が急激に全てのプロジェクトに採用されるということは少なく、プロジェクトの性質に合わせて徐々に浸透していくことがほとんどである。アジャイル開発はその性質上、セキュリティのための修正にもスピードが要求されるので、手戻りをなくすために問題の早期発見がより重要となる。したがってセキュリティのレビューも、ウォーターフォール型開発で一般的な、完成後のセキュリティレビューやペネトレーションテストではなく、開発時におけるコードレビューや静的コードスキャンを自動的に行う、いわゆる「シフトレフト」が求められる。DevOpsにこうした自動的なセキュリティチェックを取り入れた、DevSecOpsの概念が提唱されているが、本稿では自動化やツールの導入の観点ではなく、こうしたセキュリティチェックをも自動化した開発においてセキュリティ担当者が果たすべき役割について説明する。

図表15：セキュリティチェックのシフトレフト

・従来のウォーターフォール型開発では各フェーズの終了時にセキュリティのチェックを行っていたが、
アジャイル開発では構築中に都度チェックを行う必要がある。
チェックが前工程（左）に移行していくことから、シフトレフトと呼ばれる。



2.セキュリティ担当者は「ゲートキーパー」から「アジャイルの輪の中への参加」を

アジャイル開発におけるセキュリティ担当者の役割の変化をまとめると、以下の3点になる。

1. 開発者の啓蒙と教育
2. 適切なセキュリティチェックプロセスとツールの導入
3. Trust, but Verify

1. 開発者の啓蒙と教育

開発されるアプリケーションのセキュリティは、開発者によるコーディングに大きく依存する。しかし、高度に自動化され、高速なリリースが要求されるアジャイル開発においては、全てのコードをセキュリティ担当者がレビューするのは不可能である。したがって、通常はセキュリティに疎遠な開発者を啓蒙し、教育することが、セキュリティ担当者の重要な役割の1つとなる。これまではゲートキーパーとしてリリース前の判定会議でしか顔を合わせないという関係性だったとしても、開発現場に足を運んでアジャイル開発の輪の中に入り、啓蒙活動を行うという変化が求められる。

2. 適切なセキュリティチェックプロセスとツールの導入

DevSecOpsというとどうしてもツールの導入が先行する印象があるが、いきなりツールを導入することはおすすめできない。使い慣れないツールや結果を生かせないツールを入れても開発者に利用されず、無駄な投資になる恐れがあるからである。まずは自社の開発するアプリケーションや開発者のレベル、開発体制などを俯瞰した上で効果的なセキュリティチェックプロセスの策定を行い、その上で必要な箇所にツールを実装するアプローチが望ましいと考える。多種多様なアプリケーション開発環境において常に最適なプロセスやツールはないため、原則とリスクの受容を使い分ける判断ができる関係を築いておくことも重要である。

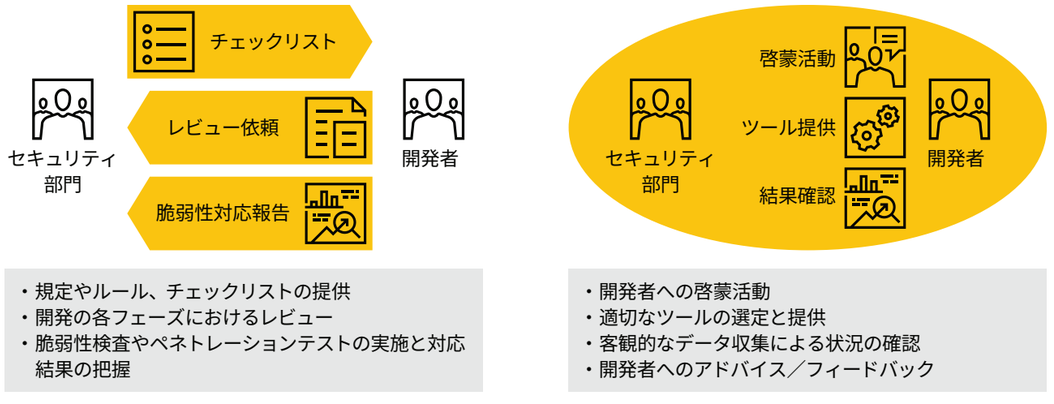
3. Trust, but Verify

前述の通り、アジャイル開発ではアプリケーション開発者が担う役割が大きく、セキュリティ担当者が全てをチェックする事はできない。基本的にはアプリケーション開発者を信じる（Trust）ことが重要であるが、結果を常に確認する（Verify）ことも重要である。チェックリストを作って自己申告してもらった結果を確認するのではなく、静的解析ツールの実行結果および修正状況やペネトレーションテストの実施結果など、客観的なデータを確認し、状況を常に把握することが必要となる。

本章では、大企業でのアジャイル開発におけるセキュリティ担当者の役割の変化について述べた。大企業でアジャイル開発に取り組む場合、これまでアプリケーション開発を担っていたベンダー／協力会社とは異なる企業と協業して開発を行う事例も多く、そうした新規の協力会社は社内のレビュープロセスなどに関する知識も少ないため、どうしてもセキュリティ担当者の目が行き届かなくなりがちである。アジャイル開発が広まっていくに連れ、セキュリティ担当者はこれまで以上に現場に飛び込んでいかなくてはならないことを理解し、実践していただきたいと思う。

図表16：セキュリティ担当者の役割の変化

・セキュリティ担当者は開発フェーズにおけるゲートキーパーからアジャイル開発のアドバイザーに役割を変化させなければならない。



3. アジャイル開発でのセキュリティ実装 インフラ担当者の役割

1. アジャイル開発環境を支えるインフラ技術 ――サーバーレスアーキテクチャや コンテナ技術の台頭

近年、クラウド上ではさまざまなサーバーレスアーキテクチャやサーバーレスコンテナ技術が登場している。こうした環境では、利用企業が自分たちでOS環境をメンテナンスする必要がない。こうした技術はDevOpsやアジャイル開発と相性がよく、コンテナ技術の進歩も相まって、OSレイヤーは実行環境の一部として、アプリケーションと一緒にデプロイされるようになりつつある。さらにインフラ構成管理ツールにより、インフラのデプロイも自動化することが可能となっており、かつてのようにインフラ担当者のみがOSにログインできる特権を持ち、アプリケーション開発者の依頼に基づき作業を行う、という場面が徐々に減りつつある。

2. 存続し続ける既存システムとアジャイル環境を両立させるアーキテクチャ設計・導入を

アジャイル開発におけるインフラ担当者のセキュリティ上の役割は、主に以下の2点に集約されると考える。

1. セキュリティを考慮したインフラアーキテクチャの設計と導入
2. 脆弱性の管理とセキュアな構成の提供

1. セキュリティを考慮したインフラアーキテクチャの設計と導入

セキュリティを考慮したインフラアーキテクチャの設計と導入において重要なのは、いきなり全ての環境がクラウドやコンテナに移行するわけではないということである。大企業においてはレガシーな基幹システムや既に構築されたプライベートクラウドが存在するため、そうした環境を併用しながら徐々に新しいアーキテクチャに移行していくのが常である。したがって、アプリケーション開発者が求めるアジャイルなインフラを導入するにあたり、既存環境との親和性やセキュリティを考慮したアーキテクチャを設計し、導入することが重要な役割となる。

その際には、採用する技術の特性を踏まえた、これまでとは異なる運用面での考慮が必要である。例えば、既存環境では踏み台サーバーを経由してホストOSに管理者アカウントでログインして実行していた作業を、インフラ構成管理ツールを使って自動デプロイさせることで管理者アカウントの使用を禁止するなど、これまでとは違った考え方が必要になる。こうしたアーキテクチャを導入することで、アプリケーション開発者はインフラの構成に頭を悩ますことなく、開発に集中することができる。

2. 継続的なセキュリティを実現する「脆弱性の管理」と「セキュアな構成の提供」

これまではOSやミドルウェア層の脆弱性についてはインフラ担当者が情報を収集し、パッチを適用することで管理がなされてきた。先ほど述べたように、アジャイル環境と既存環境の併用が続く以上、既存環境向けのこうしたセキュリティ運用が無くなることはない。さらに実装形態によっては、コンテナはホストOSの上にデプロイされることもあるため、ホストOSの管理は引き続きインフラ担当者の業務範囲に含まれると考えられる。

こうした環境においては、インフラ担当者とアプリケーション開発者の役割分担が曖昧になってしまうため、たとえインフラ層がアプリケーションの一部としてデプロイされるとしても、その構成や設定に不備がないかをインフラ担当者がチェックすることを推奨する。脆弱性が発見されればアプリケーション開発者と情報を共有して対応することが重要であるし、セキュリティが確保されたセキュアな構成情報を提供することが必要になる。

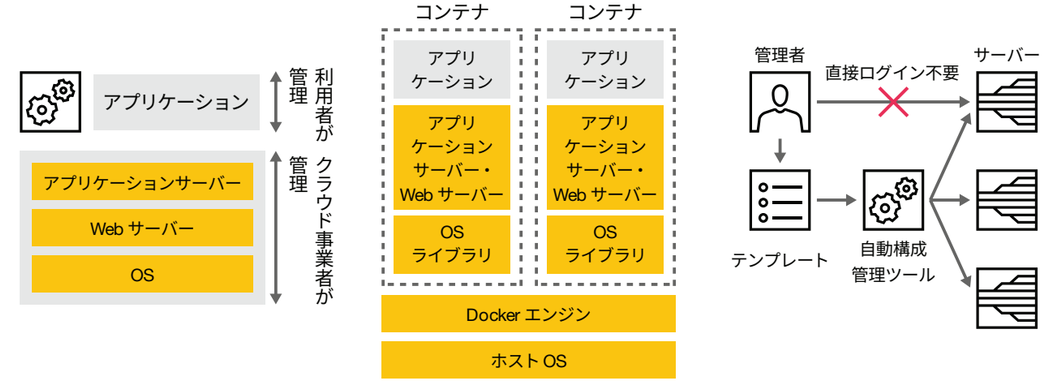
また、アプリケーション開発者がデプロイしたコンテナの設定を確認することも重要になる。たとえアプリケーション開発者により維持・管理されるとしても、開発したアプリケーション・コード以外の部分でインフラ担当者が担う役割は依然として大きい。

本章ではアジャイル開発におけるセキュリティ担当者とインフラ担当者の役割の変化について述べてきた。アジャイル開発では、アプリケーション開発者が主役でセキュリティ担当者とインフラ担当者は蚊帳の外もしくはスピードを阻害する抵抗勢力と見なされてしまう事例も散見される。しかし、いかにアジャイルなアプリケーション開発ができようともセキュリティは無視してはいけない要素であり、それに対するセキュリティ担当者とインフラ担当者の役割は、変化こそすれ不要となるものではない。

大企業においては役割分担が進んでおり、全ての領域を1人の開発者がカバーすることは不可能である。ぜひ変化を取り込み、自らの役割を再認識した上で、協力してアジャイル開発におけるセキュリティを向上させていただきたいと思う。

図表17：アジャイル開発を支えるインフラ技術

・サーバーレスアーキテクチャやコンテナ技術などはアジャイル開発と相性がよく、
これまでのようなインフラ担当者とアプリケーション開発者の役割分担の垣根が曖昧になりつつある。



図表18：インフラ担当者の役割と変化

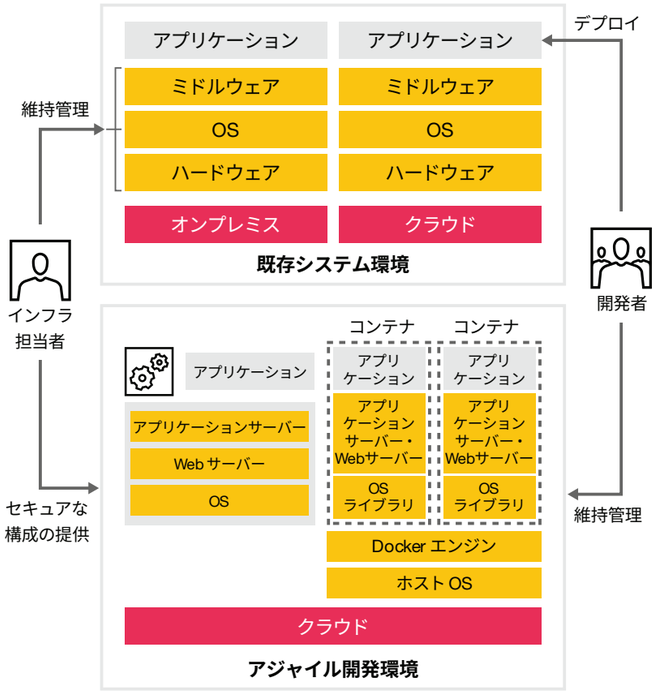
・存続する既存システムと新しい技術を取り込んだアジャイル開発環境を両立させるアーキテクチャ設計と、継続的なセキュリティを実現する脆弱性管理およびセキュアな構成の提供が主な役割となる。

インフラアーキテクチャの設計と導入

- 既存環境とアジャイル開発環境双方を見越したインフラアーキテクチャの全体設計
- それぞれの特性に合わせたセキュリティ施策の検討と導入

脆弱性の管理とセキュアな構成の提供

- 脆弱性情報の管理と対応実施
- セキュアな構成情報の提供
- 稼働中の環境の構成チェック



3 CSIRTを進化させる次の一手

1. 攻撃者を欺く攻めのセキュリティ技術、サイバーデセプション

サイバー攻撃の驚異的な進化に対し、防御する企業や組織は後手に回っていると言わざるを得ない。従来のサイバー攻撃対策は、それを迂回する攻撃手法が台頭すると無力に等しくなるという致命的な弱点を抱えており、防御側は新しい攻撃手法に一つずつ対処していくほかないのが実情である。

このような状況を打破すべく、「アクティブディフェンス」という理念が企業に求められつつある。これは、サイバー攻撃の都度対策を講じる受動的な取り組みではなく、能動的に攻撃者にアプローチする考えを言う。今回は、この手法の一つである、攻撃者を罠にかけて捕捉する「サイバーデセプション」について紹介する。

1. サイバーデセプションとは

サイバーデセプション（以下、デセプション）は直訳すると「欺くこと」を意味し、その言葉通り、ネットワーク内に配置した罠（偽の情報など）を用いて攻撃者を欺き、攻撃を遅延・阻止する手法を指す。「デコイ」（囮）と呼ばれるこの罠は実際に利用されるサーバーやサービス、アプリケーションなどを模しており、それを罠と知らずに触れた攻撃者を検知する仕組みであるため、サイバー攻撃が進化したとしても、その効果が陳腐化することはない。

囮を利用するという点において、デセプションと類似した技術に「ハニーポット」がある。ハニーポットは古くから存在する技術であり、一般的には誰でもアクセスできるインターネット空間に設置され、主に攻撃の内容の偵察や調査・分析に用いられてきた。それに対してデセプションは、攻撃の検知や遅延を目的に、組織の内部ネットワーク環境に設置する。ハニーポットの応用型と言うことができるであろう。

2. デセプションの仕組み

ここからは、デセプションの仕組みを具体的に見ていこう。簡単な例として、企業の業務用端末に罠を仕掛けるケースを説明する。

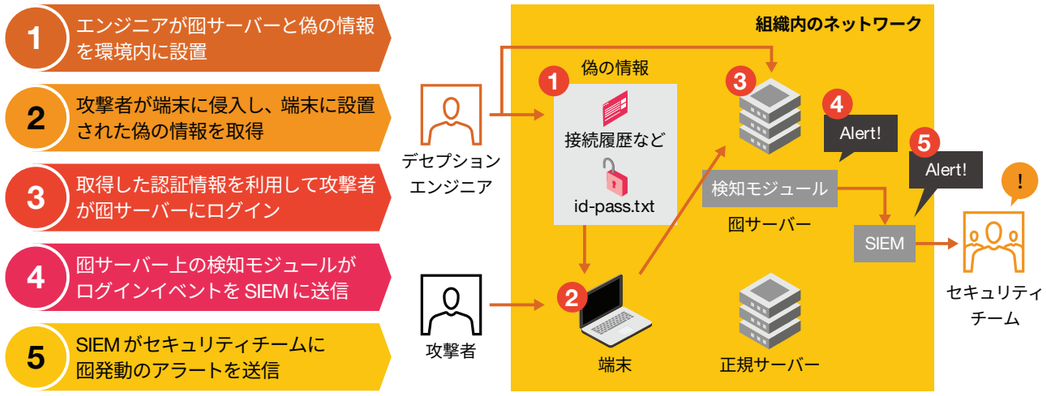
攻撃者は、端末上にパスワードを含むアカウント情報が記されたファイルを発見すると、その接続履歴などを駆使して当該アカウントの悪用を試みると考えられる。デセプションは、その攻撃者の行為を逆手にとって、あらかじめ偽のアカウント情報を記したファイルを囮として配置し、この情報が悪用された場合に検知する。

当然ながら、実際のデセプション環境はより複雑で、さまざまな罠を幾重にも配置し、攻撃者を確実に罠にはめる巧妙な仕組みが必要である。企業や組織のITシステム環境において成立し得る攻撃シナリオに基づき、特定のコマンドやスキャン行為に対して偽の情報を返答するモジュールや、SIEM（Security Information and Event Management）などを活用してデセプション環境を構築するといった対応が求められる。以下にその流れを記す（図表20）。

図表19：デセプションとハニーポットの相違点

	デセプション	ハニーポット
実装の目的	攻撃の兆候の検知、遅延	攻撃の調査、分析
主な設置環境	組織の内部ネットワーク環境	公開システム環境（インターネット）
囮への誘導方法	組織の内部ネットワークに罠（偽の情報など）を仕掛ける	なし（攻撃されるのをひたすら待つ）
有効な攻撃段階	侵入拡大	偵察

図表20：偽の情報と囮サーバーを利用したデセプション環境と攻撃検知の流れ



3. デセプションの効果

あらためて、デセプションを利用することで期待できる効果を整理する。

セキュリティ態勢の向上

デセプションは、攻撃手法の新旧にかかわらず、企業や組織のシステム内に侵入した攻撃者の活動に対する気づきを与え得る、組織全体のセキュリティ態勢の向上が期待できるソリューションである。また、囮となる情報やサーバーは正規のシステムに基本的に干渉しないため、導入後の運用負担が軽く、誤作動などによる企業活動への影響も少ないという特長もある。

インシデント対応能力の強化

囮となる情報に導かれた攻撃者の活動は正常な企業活動と明らかに異なるため、非常に高い精度で攻撃を検出し、分析することが可能である。また、アラートの精度が高いことから攻撃の内容や被害状況を推測しやすいため、アラートごとにどう対処するのか、手順を事前に整備することができる。

サイバー攻撃被害の軽減

正規のサーバーを模した囮サーバーを利用すると、攻撃者がそこに留まっている間は正規のサーバーへの攻撃の拡大を抑えられ、攻撃への対処に向けた猶予時間を稼ぐことができる。

4. デセプションの導入時に考慮すべき2つのポイント

ここまではデセプションのメリットを語ってきたが、安易に導入することで、かえってサイバー攻撃を活性化させてしまう可能性がある。最後に、私たちが考える導入時における考慮事項を紹介する。

有効な囮の選択

企業や組織によって保護すべき情報資産やシステムの環境は異なり、攻撃の手法や侵入経路も変化する。そのため、組織によって有効な囮の種類や設置するポイントは異なってくる。自組織で発生し得るリスクシナリオを定義・評価し、その結果を踏まえて最適なデセプションの方法を選択することが重要である。

事前のリスク確認の徹底

囮サーバーは攻撃者にアクセスされることを前提としているため、囮サーバーやその周囲の環境が脆弱な場合、デセプションがセキュリティホールとなる可能性がある。デセプションが被害拡大のきっかけとならないよう、前述のリスクシナリオ評価と合わせてペネトレーションテストをはじめとする準備を行い、リスクがないかを確認した上で導入する必要である。

デセプションは従来のセキュリティを強化するものであり、それ単体で完全なセキュリティを担保するものではない。攻撃者の侵入を未然に防ぐ対策を講じた上で、仮にそれらのセキュリティが突破された時のための対策であることに留意されたい。

2. 「サイバーセキュリティ資産管理」によるCSIRTパフォーマンスの最大化

1. あらためて問う、資産管理の重要性

企業における情報セキュリティマネジメントでは、CSIRT（Computer Security Incident Response Team）をはじめとする専門組織の設置を通じてセキュリティ機能が「集約」され、インシデントレスポンス態勢の高度化を実現しているケースが多く見られる。一方、この機能集約という業務面の整備のみが先行し、その機能の遂行に求められる保護すべきIT資産の管理は、依然として各組織に「分散」されている場合も少なくない。

このねじれた構造がセキュリティマネジメントにおける業務負担やコストの上昇、また活動自体の効率性や敏捷性に課題を生じさせている。

サイバー攻撃が高度化し、ビジネスの急速なデジタル化によって保護対象が増加・多様化する現在そして未来においては、CSIRTはこれまでよりもクイックに業務サイクルを回し、組織の安全性を担保し続ける必要がある。こうした取り組みを実現するためには、IT資産の管理情報を一元的に集約すると共に、セキュリティ機能と資産管理の主体のねじれを解消してCSIRT活動のパフォーマンスを最大化する「サイバーセキュリティ資産管理」（CSAM：Cyber Security Asset Management）が必須基盤と考える。今回は資産管理の現状と課題をあらためて見つめ直し、サイバーセキュリティ資産管理がなぜ必要なのかを考察する。

2. 現状の課題――CSIRT活動を阻害する分散化された資産管理

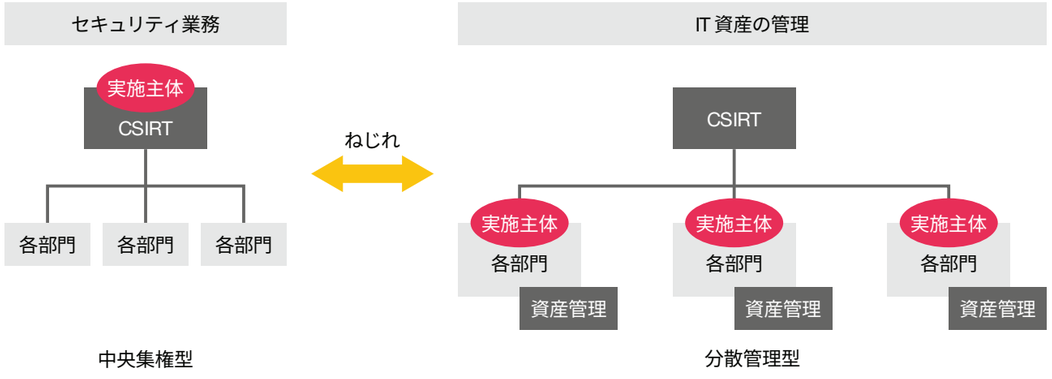
セキュリティ機能と資産管理のねじれ構造は、CSIRTが保護すべき資産の詳細を把握していないこと、また必要な情報にアクセスするまでに時間と労力を要していることを示している。これは企業や組織に、次のような課題を生じさせる。

セキュリティリスクの放置

CSIRTが各組織・各資産の抱えている脆弱性やセキュリティリスクを把握できていないために必要な対策を講じられず、セキュリティリスクが放置される危険がある。

また、各組織に委ねられた資産管理の品質にCSIRT活動が依存するため、管理漏れが生じた場合、CSIRTはセキュリティ機能を全く提供することができない。

図表21：セキュリティ機能と資産管理のねじれ



セキュリティ業務効率の悪化

CSIRTが各組織の資産管理情報にすぐにアクセスできないことで、CSIRT活動に必要な情報の入手に時間を要し、また関係者を幾重にも巻き込むなど、業務効率を悪化させる可能性がある。

例えば、インシデント対応時に、対処法の判断に必要な情報が手元で管理できていない場合、担当者へのヒアリングや実機へのログインを伴う調査が必要となり、インシデントへの対処・封じ込めに時間を要する。サイバーセキュリティ資産管理を導入し必要な情報を恒常的に管理することで、情報収集における時間が大幅に削減し、迅速な対処・封じ込めを実現することができる（図表22）。

3.「サイバーセキュリティ資産管理」の導入に向けて

ここからは、CSIRT活動に必要となる情報を即時的かつ漏れなく収集・管理するサイバーセキュリティ資産管理をいかに実現するかを考える。CSIRT活動に必要な情報は多岐にわたるため、情報収集・管理の設計に不備があると、期待する効果が得られないだけでなくサイバーセキュリティ資産管理自体の負荷が高まる恐れがある。

まず設計で重要なことは、目的を達成するために必要な、管理すべき情報を定義することである。この際、業務単位で、その開始から終了までに必要な情報を詳細に洗い出し、システムの重要性や費用対効果を考慮の上、サイバーセキュリティ資産管理においてどの粒度まで情報を管理するかを決定する。

例えばインシデント対応業務では、部門からの相談・報告、トリアージ、対処・封じ込めといった各工程で異なる情報を取り扱う。どのような情報を管理するべきかについては、システムごとの重要性や特性に鑑み、どの工程まで業務効率を改善するべきかを検討することで導くことができる（図表23）。

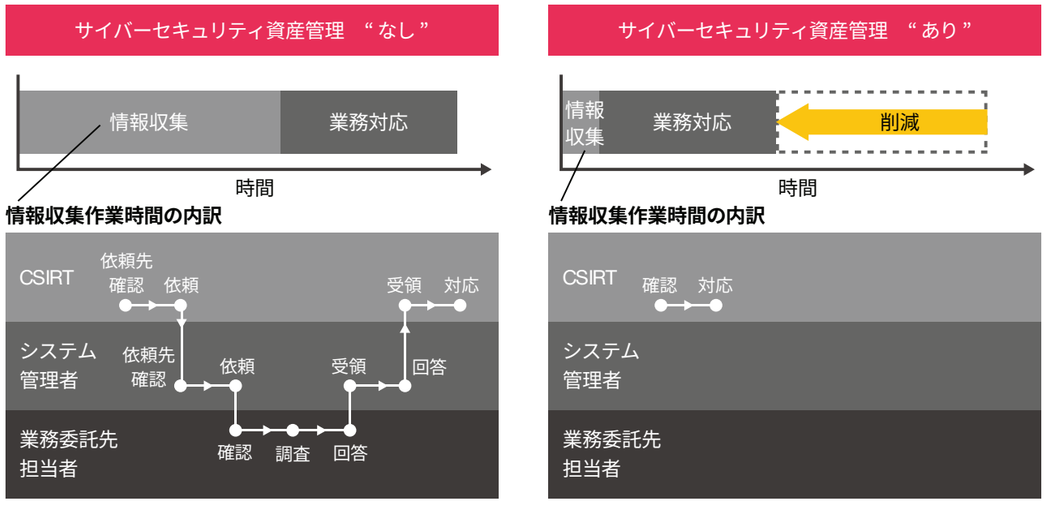
また、必要な情報の収集方法を検討することも重要である（図表24）。

サイバーセキュリティ資産管理で管理する情報は、「静的な情報」と「動的な情報」に分類される。「静的な情報」とは、システムの運用時にほぼ変更がない情報（各種連絡先や属性など）を指し、各部門へのヒアリングや棚卸によって収集可能である。

一方、「動的な情報」とは、システムの運用時に頻繁に更新される情報（バージョン情報やオープンポート、起動プロセスなどのステータス情報）を指す。これらの情報は、陳腐化することのないよう、情報収集を自動化することが望まれる。

その他、サイバーセキュリティ資産管理自体のアクセス管理といったセキュリティに係る事項や、収集した情報を業務に還元する活用方法の検討も欠かせない。

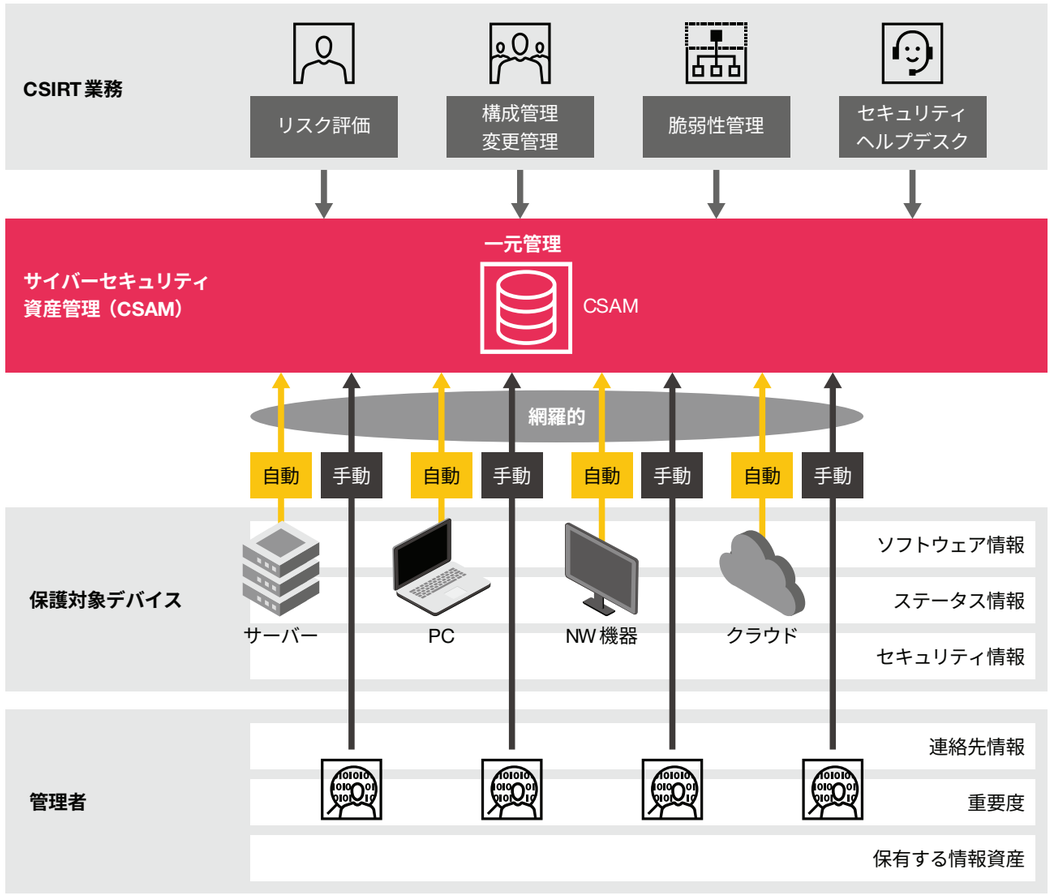
図表22：サイバーセキュリティ資産管理の有無で変わるインシデント対応方法（イメージ）



図表23：インシデント対応における情報の整理

インシデント対応業務		情報管理の方針		
工程	必要な情報	公開系システム	社内システム（重要）	社内システム（一般）
連絡・報告	・連絡先 ・担当者 ・IP アドレス ・ホスト名	○（手動）	○（手動）	○（手動）
トリアージ	・システムの重要性 ・保有する情報の機微性 ・業務用途	○（手動）	○（手動）	○（手動）
対処・封じ込め	・OS・ソフトウェア情報 ・平時の起動プロセス ・平時のオープンポート番号 ・AV パターンファイルのバージョン	●（自動）	●（自動）	×
サービス停止判断	・判断者 ・停止条件 ・停止時の連携先 ・停止に影響をうける業務	○（手動）	○（手動）	○（手動）

図表24：サイバーセキュリティ資産管理における情報の収集・管理方法



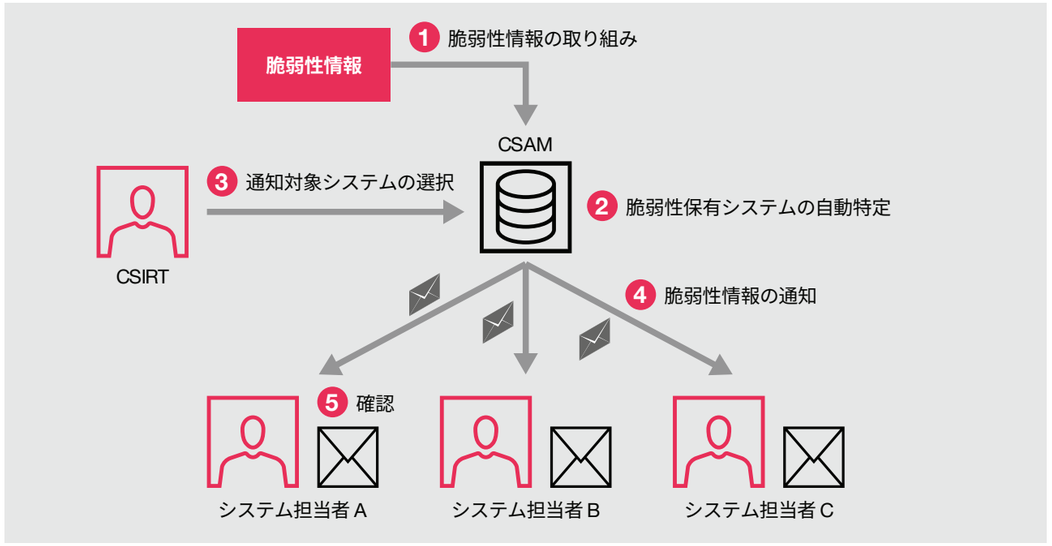
4. サイバーセキュリティ資産管理で向上するCSIRTパフォーマンス

サイバーセキュリティ資産管理を活用することで、CSIRT活動の飛躍的な向上が期待できる。単純なケースでは、ソフトウェアの利用有無やバージョン情報が一元管理できると、セキュリティ製品（IPS／IDS、WAF、AVなど）やSOC（Security Operation Center）による検知イベントへの影響の有無や、新たに公開された脆弱性情報に対する影響を、短時間で正確に把握できる。さらに、脆弱性の自動特定から通知、対応管理までのプロセスをサイバーセキュリティ資産管理で実現すると、インシデントの発生防止にも大きく寄与することができるであろう（図表25）。

多くの企業では、セキュリティ監査の名目で年次で担当者に膨大な設問が投げかけられることに「業務負荷が高い」といった不満の声が上がっている。この課題も、サイバーセキュリティ資産管理によって各システムから収集した情報を活用し、設問数を削減することで軽減・解消が可能である。さらに、サイバーセキュリティ資産管理で収集したシステムの設定や環境値と期待値との比較を自動化することで、セキュリティ監査の自動化だけでなく、新たに構築されるシステムに対しても、そのセキュリティ対策状況を評価することができるようになる。

これまでの資産管理の域を超えて情報システムをセキュリティ目線で一元管理し、業務を最適化する。そうすることで、保護対象のシステムが増加・多様化しても持続可能なセキュリティ態勢が構築でき、CSIRTの体制整備のみならず、さらなる機能活性化への礎となることであろう。

図表25：サイバーセキュリティ資産管理を活用した脆弱性管理



3. 再考、スレットインテリジェンス

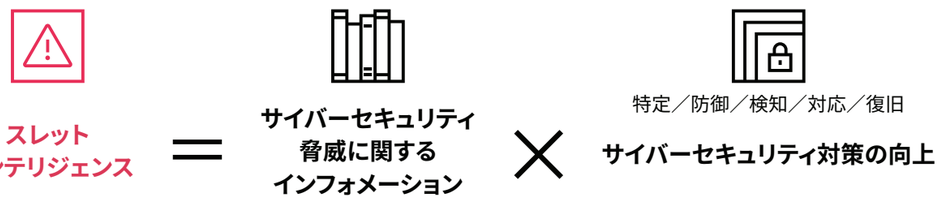
1. スレットインテリジェンスを「意思決定の知見」として活用するために

近年、スレットインテリジェンスまたは脅威インテリジェンスと呼ばれる情報および情報提供サービスが注目を集めている。以前からCVE（Common Vulnerability Enumeration）に代表されるソフトウェア脆弱性に関する情報を提供するサービスは存在している。また、IoC（Indicator of Compromise）のように実際のサイバー攻撃で悪用されたマルウェアのハッシュ値や通信先IPアドレスなどを提供するサービスも近年登場している。こうした取り組みとスレットインテリジェンスはどこが違うのであろうか。

インテリジェンスは一般的に、インフォメーションを特定の目的で分析して得られる意思決定のための知見を意味する。そのためインテリジェンスを語る上で「分析の目的は何か?」は欠かすことができない問いと言える。スレットインテリジェンスは、文字どおりサイバーセキュリティ脅威に関するインフォメーションを対象とし、自組織のサイバーセキュリティ対策向上を目的とした分析により得られた、意思決定のための知見と考えることができる。サイバーセキュリティ対策という概念をどのように捉えるかにはさまざまな考え方があるが、代表的なものとしてはNISTサイバーセキュリティフレームワーク（NIST CSF）が挙げられる。そのため同フレームワークを構成する5つの要素（「特定」、「防御」、「検知」、「対応」、「復旧」）それぞれの観点からサイバーセキュリティ脅威に関するインフォメーションを分析したものが、スレットインテリジェンスと考えることができる。

「スレットインテリジェンスサービスが有用だと聞いてと契約したが、有効な使い方が分からない」という声を聞くことがある。こうした場合、「どのようなセキュリティ課題を改善するか・高度化するか」という課題・目的の設定、そのためにどのような知見が必要か、知見を得るためにはどのような情報・分析が必要か、という検討プロセスがおろそかになっていることが少なくない。冒頭の脆弱性情報の場合、「自社システムに関連する、深刻度の高い脆弱性情報の把握」、「自社システムに関連する、実際の攻撃での悪用が確認されている脆弱性情報の把握」、「自社システムに関連する、同業他社を狙った攻撃が確認されている脆弱性情報の把握」では分析の目的が異なり、必要となる知見や情報も異なる。インテリジェンスが「意思決定のための知見」であることを踏まえると、企業や組織においては、徹底して自組織で活用することを前提とした目的設定が必要だと言える。

図表26：スレットインテリジェンスの定義



2. 乱立するスレットインテリジェンスサービスとその分類

昨今、さまざまなスレットインテリジェンスサービスが提供されている。冒頭の脆弱性情報やIoC、APT（Advanced Persistent Threat）の詳細解析情報、ダークウェブのモニタリング情報、地政学リスクとサイバー攻撃の分析情報など、内容は多岐に及ぶ。こうしたスレットインテリジェンスサービスの全体像は、次の3つに大きく分類することができる。

ストラテジック型

政治・経済・社会・技術などのマクロ要因とサイバー攻撃の関係性を分析し、情報提供するサービス。実際に発生したサイバー攻撃の背景、攻撃者像、各国・組織のサイバーセキュリティ関連動向の分析を行うことで、将来的に想定されるサイバー攻撃のリスクを洗い出す。

OSINT（Open Source Intelligence）型

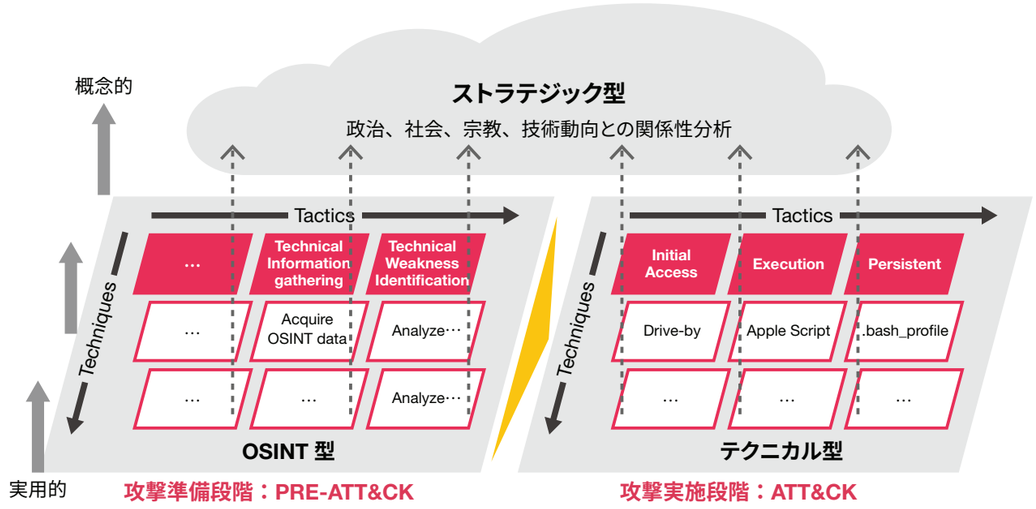
ダークウェブを含むインターネット上の公開情報を対象として、情報を収集・分析し、情報提供するサービス。サイバーセキュリティ対策を行う上で認識すべき脆弱性情報、漏えい情報、攻撃の予兆、インターネットに露出したShadow ITデバイスなどの攻撃者にとって有益な情報を提供する。攻撃者から見た場合、攻撃準備段階に相当する（MITRE-PRE-ATT&CKで説明される戦術に相当）。

テクニカル型

実際に発生したサイバー攻撃やAPTを詳細に解析し、情報提供するサービス。最新の攻撃手法を明らかにし、その対策や攻撃に関連したIoCなどを提供する。攻撃者から見た場合、攻撃実施段階の手口に相当する（MITRE-ATT&CKで説明される戦術に相当）。

こうしたスレットインテリジェンスサービスを活用するためには、前述のとおり、分析の目的が明確になっていることが重要である。サービス側で必要な分析が行われており、提供される情報が自組織にとって必要な知見である場合は、追加の分析は必要ない。一方で業界または自社特有の情報、特性を考慮する必要があるといった理由でサービス側での分析が不十分な場合は、追加での分析が必要となるため、事前にアウトソース・インソースする内容を見定めておくことが必要である。

図表27：スレットインテリジェンスの全体像



3. CSIRTでスレットインテリジェンスをどう活用するか

CSIRTでのスレットインテリジェンスの活用を考える場合、外部のスレットインテリジェンスサービスの利用有無、インソースでの追加分析の有無に関わらず、分析により得られた知見を活用するためには、既に一定水準でCSIRTの活動が定義・運営されている必要がある。

この前提において、初めに自組織のCSIRTがサイバーセキュリティ対策のどの機能を担うのかを明らかにする必要がある。例えば、NIST CSFの一要素である「特定」を考えた場合、P29【「サイバーセキュリティ資産管理」によるCSIRTパフォーマンスの最大化】でも紹介したように、IT資産管理が各業務部門に分散しているケースもあれば、サイバーセキュリティ資産管理の導入により必要な情報がCSIRTにより管理されているケースも考えられる。また、「対応」「復旧」についてもCSIRTが中心になるケース、インシデントが発生した事業部門が中心となるケース、インシデントに応じて組成された対応組織が中心となるケースなどが考えられる。そのため、まずはCSIRTが行う活動において存在する課題、高度化が必要となる項目を明らかにし、分析の目的を設定する。一例を以下に示す。

- 自組織のビジネス戦略に基づいて採用するIT技術に対してどのような攻撃が行われているのか、想定されるのかを明らかにする。これにより、「防御」「検知」の仕組み、対応体制を準備する。
- 自組織の資産管理から漏れているShadow ITを特定する。これによりShadow ITへの対策を促す。
- 自組織に関する漏えい情報、漏えい時期、漏えい元を特定する。これにより見逃していたインシデントを特定し、被害範囲の把握、原因究明、再発防止策を実施する。また、外部サイトからの情報流出の場合は、利用サービスの見直し、選定基準の改訂などを促す。
- 同業他社を狙った最新の攻撃手法を把握する。これにより、導入すべき検知、防御の仕組みを明らかにし、対策を実施する。
- 日々発見される脆弱性について、実際に自社への攻撃が想定される脆弱性を特定する。これにより、当該脆弱性について例外的な対処を行う。

上記の例は、現実には一筋縄ではいかず、課題として認識されているものの改善されないまま放置されていることが少なくない。スレットインテリジェンスは「自組織の意思決定のための知見」である以上、自組織固有の特性を含んでおり、異なる組織間で共通して活用できることはあっても、それが一般化されることはない。「目の前にある情報をどう有効活用するのか」ではなく、問いに相当する「分析の目的」の設定と、その答えに相当する「実装と運用」のサイクルを継続的に回し、双方のレベルを段階的に上げていく必要がある。

4. インシデントの発生を前提とする時代 サイバーセキュリティプレイブックの整備

サイバーセキュリティの施策や投資と言えば、セキュリティインシデントの発生に対する「予防」策や「検知」策を中心とする企業が多く、発生し得るインシデントへの「対処」を改善するための施策や投資は、まだ一部のセキュリティ先進企業に留まってしまっているのが現実である。サイバーセキュリティ対策の考え方の主流は、「インシデントを予防する」ではなく、「インシデント発生を前提として対策する」にシフトしており、インシデントへの「対処」についてあらためて検討を行うべき時期に来ていると言える。今回は、インシデントへの「対処」を強化するためのツールである「サイバーセキュリティプレイブック」を整備するポイントについて解説する。

1. サイバーセキュリティプレイブックとは

サイバーセキュリティプレイブック（以下、プレイブック）は、サイバーセキュリティインシデント発生時に「いつ、誰が、何を、どのように対応すべきか」について定めた、SOC（Security Operation Center）やCSIRT（Computer Security Incident Response Team）に向けた、より高度な手順書のことである。

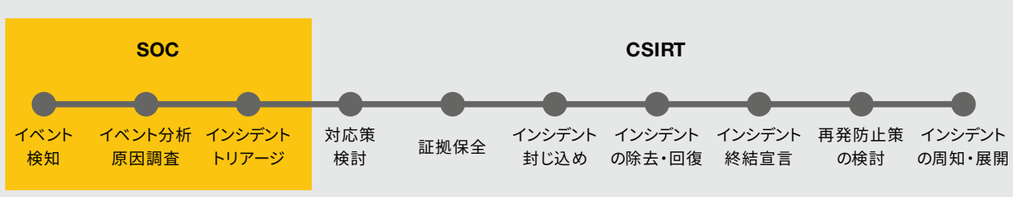
一般的に、SOC／CSIRTがサイバーセキュリティインシデントの兆候を検知した場合、次のようなフローに沿って対応が行われる。

多くの組織ではこのフローに基づいて、共通の調査手順や対応手順を定めていることであろう。しかしこの手順は、果たしてどこまで機能するのであろうか。

実際のインシデント発生現場では、発生したインシデントの性質、あるいは刻々と変化する状況に合わせて臨機応変に対処することが求められ、共通の調査手順は機能しないことがほとんどである。代表例として、情報漏えいの疑いによる調査では事実確認や原因調査が優先され、ランサムウェアの感染では、感染拡大の防止を目的にインシデント封じ込め（嫌疑端末の隔離）が優先される。また、こうした臨機応変な対応は、十分な知識と経験を持つ上級のアナリストによって判断されることが多く、俗人化しているがゆえに、上級アナリストの不在時にはインシデントが深刻化し、企業に大きなダメージを与えるリスクを抱えている。

プレイブックは、自社に発生し得るインシデントの種類やそのシナリオに鑑み、それぞれの対応手順や判断のポイントおよび基準を整理したものを指す。プレイブックの整備により、経験の浅い担当者でも上級者の判断を仰ぐことなく対応ができ、また、後述のSOAR（Security Orchestration Automation and Response）によって、インシデント対応を自動化することも可能になる。

図表28：SOC／CSIRTの対応フロー例



2. プレイブック整備のポイント

先述の通り、プレイブックには自社に発生し得るインシデントの事象ごとに、漏れなくそれぞれの対応手順や判断基準が整理されていることが重要である。ここからは、どのようにしてプレイブックを整備するべきかについて紹介する。

Step1. 自社で起こり得る脅威シナリオの把握

初めに、自社で発生し得るインシデントと当該インシデントが与える影響範囲を漏れなく特定することが重要である。これには、さまざまな攻撃手法が成立し得るかといった観点からインシデントの影響を机上で評価する「脅威シナリオベースのリスクアセスメント」を用いることが一般的である。

プレイブックに記すべきインシデントを特定し、当該インシデントが与え得る影響を知ることによって、プレイブック内で確認するべきポイントや必要なアクションの概要が見えてくる。

Step2. 脅威を検知する仕組みの構築

次に、インシデントシナリオの開始、つまり攻撃の予兆を検知する仕組みを検討する。

自社で発生し得るインシデントのシナリオが把握できたとしても、それらを検知する仕組みがなければ、その後の対処に移ることはできない。一般的なインシデント検知の仕組みにはログメッセージが利用されるが、システムのステータス変化やプロセスの起動／停止、特定アカウントでのログインといった状態の変化も、攻撃の予兆を検知するためのトリガーとして活用することが可能である。

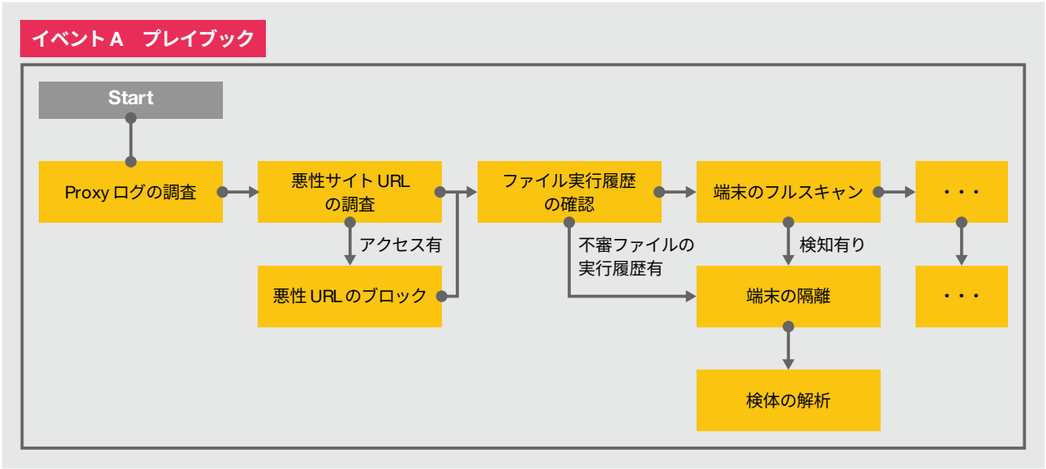
Step3. 検知後のアクションと必要な情報の整理

最後に、インシデントシナリオに基づき、プレイブック内に、取るべきアクションを整理していく。

例えば調査を行う場合は、必要な情報は何か、またその情報がどのようになっていれば期待値／異常値であるのかを整理し、次のアクション、またその次のアクションと、それぞれを有機的にひも付けて、具体的な作業内容を記載していく。

プレイブックでは、対処する要員の数も考慮しながら、システム調査などのメインストリームに並行して、当事者への聞き取りや関係者への報告などのアクションを実施し、それぞれの合流地点と各アクションにおける判断ポイントを整理しておくことが重要である。

図表29：プレイブックのイメージ（フローのみ）



3. SOARによる手順の自動化

インシデント対応においては最近、SOAR（Security Orchestration Automation and Response）と呼ばれるソリューションが注目されている。SOARでは、プレイブックに定めた手順をツール上に登録することで、その処理を自動で実行することができる。例えば、「悪性サイトへのアクセス」が疑われるイベントが発生した場合、そのURLについて、脅威インテリジェンスに関する情報を記した外部サイトなどで影響を確認し、脅威があると判断した場合、当該URLへのアクセスをURLフィルターなどと連携してブロックすることや、マルウェアをダウンロードした可能性がある場合は、当該端末の切り離しを自動で行うことができる。SOARツールの多くはあらかじめ、多くのセキュリティインシデントに対する対応手順をテンプレートとしてまとめており、当該テンプレートを自社向けにカスタマイズすれば、容易に導入することが可能である。

しかしながら、SOARは自社で発生し得る脅威を検知でき、かつその対処手順が定まっていることを前提としたソリューションである。導入したからといって即座に全てのインシデント対応を自動化できるわけではない。そのため、プレイブック整備のポイントに記載したように、リスクアセスメントなどを通じて自社で発生し得る脅威を特定し、それらを検知・調査する手順を整備した上で導入することが重要である。

プレイブックの整備は、一度手順を定めたら終わりではない。レッドチーム演習に代表されるセキュリティ診断や、実際のインシデントに対処した場合の経験や知見などに基づいて都度アップデートを行うことが必要である。そうしてプレイブックの実用性・実効性を高めていくことで、より強靭かつ属人的な対応が発生しないインシデント対応体制を築くことができるであろう。

5. 本当に必要なセキュリティ施策の導き方
――リスクスコアの算出フレームワーク活用術

限りある予算・人的リソースを踏まえて、次の一手として何をすべきか――。CSIRTの現場の多くでは、優先すべき施策について意見が割れているのが実情である。

セキュリティ対策が不十分という認識を持つ企業や組織は、各種法令やガイドラインを頼りに基本的なセキュリティ機能の整備を行っていることであろう。一方、各種法令やガイドラインで求められる基本的なセキュリティ機能を具備した企業には、次の一手を導く万能な教科書はないため、自社のビジネスや組織、保有資産や施策導入状況などに鑑み、講じるべき施策を自ら選択する必要がある。この選択の際に重要なことは、サイバー攻撃への対処、セキュリティガバナンスの強化、あるいはセキュリティ業務負荷の解消といった性質の異なる課題であっても、その課題が持つ「リスク」を見極め、優先順位を設定することである。リスクを見極める「目」がなければ、費用対効果の小さい施策を講じてしまう、あるいは、施策の必要性を経営層に訴求できず導入が進まないなどといった課題に直面することであろう。

上記の解決策として「リスクスコアの算出フレームワーク」の構築・活用を紹介すると共に、次に実施すべき施策を導く方法について記載する。

1. CSIRTが抱える課題

ビジネスのデジタル化が進むに連れ、セキュリティは企業にとって重要な経営課題となった。CSIRTの活動は自ずとビジネスとの結びつきが強くなり、マネジメント層、あるいはビジネスの現場から多種多様な要望や依頼が届くようになった。一方、CSIRTの活動には、未だ企業の生産性に対する効果が見えづらいことを理由に、十分な予算や人的リソースが配分されずに、多様な要望や課題は山積したままになっているケースが少なくない。

限りある予算やリソースを何に投じるかは、CSIRT、ひいては企業にとって重要な意思決定である。しかし、CSIRTが抱える課題や要望は多岐にわたるため、同じ軸で重要性を評価することが困難である。そのため、自社にとって本当にやるべきことなのかを議論して優先順位を決定するというプロセスが不十分なまま、「説明が容易な新規ソリューション」、「他社採用の施策」、「難易度が低い保守的な施策」など、必要性を疑う施策が実行計画に含まれることもある（図表30）。

小さなリスクの対応にリソースを投じて大きなリスクが見過ごされることはあってはならない。こうした事態を避ける上で、自社の環境や既存の対策を踏まえて、リスクや効果を適切に評価するための仕組みであるリスクスコアの算出フレームワークを整備し、自社がやるべき施策の意思決定に活用することが有効である。

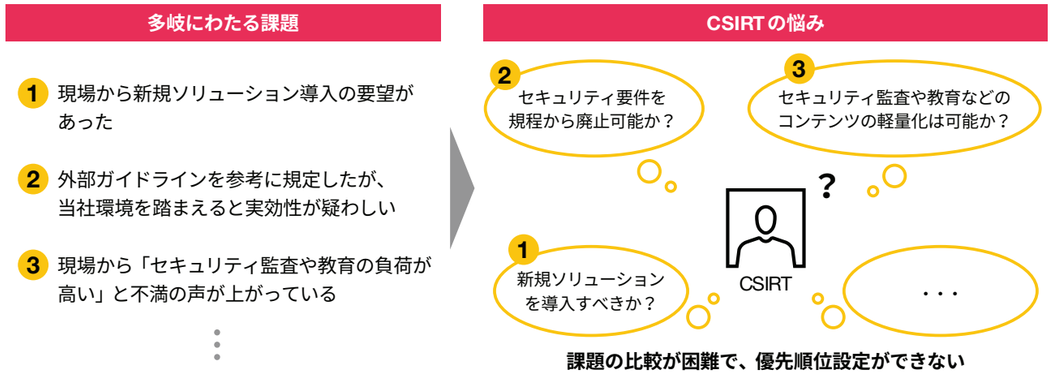
2. 「リスクスコアの算出フレームワーク」とは

リスクスコアの算出フレームワークの1つに、米国標準技術研究所（NIST）が発行する“National Institute of Standards and Technology Special Publication 800-30 rev1, Guide for Conducting Risk Assessments, September 2012”（邦題『リスクアセスメントの実施の手引き』。以下、NIST SP800-30）がある。

NIST SP800-30におけるリスクアセスメントの実施プロセスは「脅威源を特定する→脅威事象を特定する→脆弱性と素因的条件を特定する→（脅威事象が発生する）可能性を特定する→影響の大きさを特定する→リスクを判断する」から構成される。

「脅威源」「脅威事象」と聞くと、いわゆるサイバー攻撃や脆弱性情報で多く用いられる用語であることから、CSIRTが抱えるさまざまな課題を同一のフレームワークで評価することは困難に思えるかもしれない。しかし、サイバー攻撃と性質の異なるガバナンスや人材育成の問題であっても、その課題が残存すればどのような脅威事象が発生するのかをひも解くことで、そのリスクを導き出すことが可能である。リスクスコアの算出フレームワークは、多様な課題を一律の指標でリスクの大きさとして算定するツールであり、次の一手として何をすべきかを、リスクの大きさから客観的に判断できる効果を持つ。

図表30：CSIRTが取り扱う課題



3. リスクスコアの算出フレームワークの活用

リスクスコアの算出フレームワークの活用によって、前述のような講じるべき施策の優先度の決定だけでなく、CSIRTに寄せられる検討課題にも、解を見出すことが可能になるであろう。以下に例を記し、本コラムを締めくくりたいと思う（図表31）。

（1）新規ソリューションを導入すべきか？

リスクスコアの算出フレームワークを用いることで、新規ソリューションがもたらす効果、つまりソリューション自体がリスクをどの程度低減させるか、その大きさを評価することが可能になる。新規ソリューション導入の際に毎回リスク評価を行い、導入費用に鑑みながらデータとして蓄積することで、自社としての費用対効果の指標を構築することができ、施策の導入の是非を検討することができるようになる。

（2）セキュリティ要件を規程から廃止可能か？

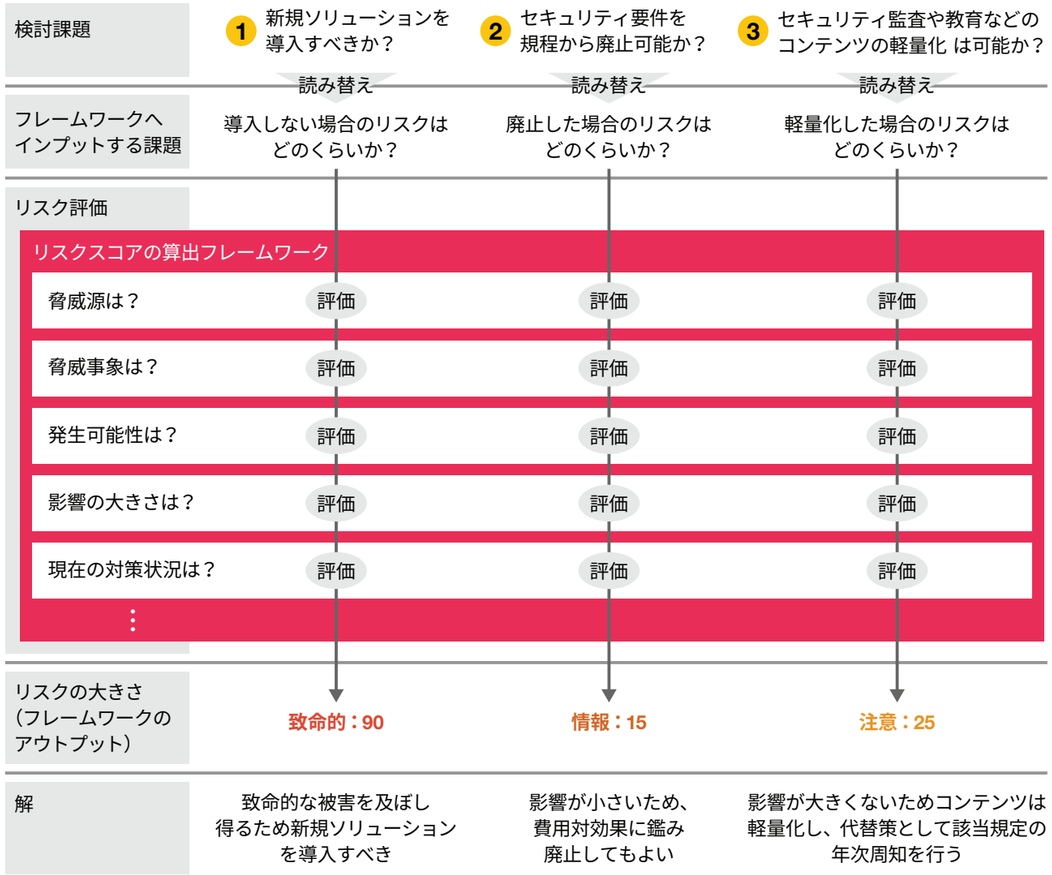
セキュリティ規程の中には、外部のガイドラインや他社事例が引用元となり、自社に鑑みるとその効果が疑わしい要件が存在している場合がある。リスクスコアの算出フレームワークで、該当する要件を廃止した場合のリスクの大きさを算出できるため、要件の持つ効果が薄いことを客観的に証明できれば、スムーズに廃止へと導くことができる。

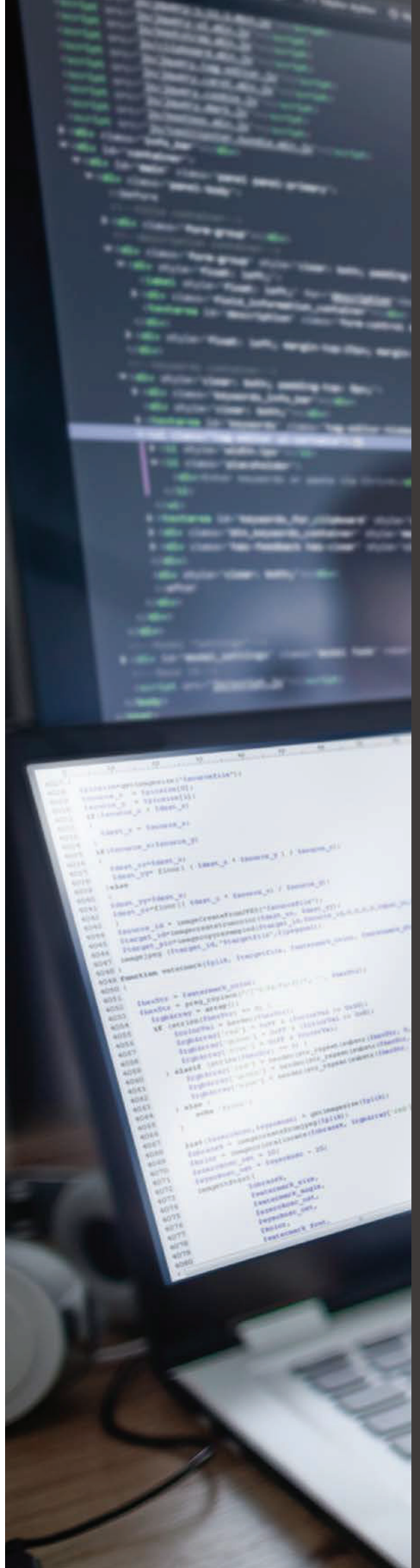
また、規定に要件を追加する場合も同様である。例えば、外部のガイドラインが求めるセキュリティ要件が、既に自社では技術的安全管理措置によってリスク低減済みであるなど、要件を追加しない場合のリスクを明らかにすることで、自社の規程に採用すべきかを判断することができる。

（3）セキュリティ監査や教育などのコンテンツの軽量化は可能か？

監査項目や教育コンテンツなどは年を追うごとに肥大化する傾向があり、対象者の業務負担を軽減するために、その分量の削減に迫られるケースがある。リスクスコアの算出フレームワークを用いることで、各コンテンツの効果を横並びに評価することができ、効果の高いコンテンツに絞り込むことで、一定の水準を保ちつつ、対象者の業務負担を軽減することが可能になる。

図表31：リスクスコアの算出フレームワークの活用





おわりに

新型コロナウイルス感染症の拡大により、ビジネスや私たちの働き方は大きく変わりました。ITインフラはキャパシティを超え、業務継続に支障をきたす企業も出てきました。そのため、製造拠点や営業拠点、海外支店からの特定のトラフィックについてはデータセンターを通さずにインターネットに直接接続するローカルブレイクアウトという手法をとることで解決を図っている企業もあります。しかし、インターネットとの接続拠点を新たに設けるということは同時にサイバー攻撃のリスクも高まることになります。

一方、サイバーセキュリティ上の脅威に目を向けると、ハッカーによる攻撃は特定の企業に確実にダメージを与えるためにより高度化してきました。

変わりゆくビジネス環境、そして高度化されたサイバー脅威により、私たちはサイバーセキュリティに対するこれまでの概念を改めなくてはなりません。本稿でご紹介した新しいポリシーを受け入れ、ITインフラの大きな変革への一歩を踏み出す時がきています。

お問い合わせ先

PwC Japanグループ
https://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 パートナー

【執筆者】

辻 大輔
PwCコンサルティング合同会社 ディレクター

小林 公樹
PwCコンサルティング合同会社 ディレクター

村上 純一
PwCコンサルティング合同会社 ディレクター

神野 光祐
PwCコンサルティング合同会社 シニアマネージャー

田村 郷史
PwCコンサルティング合同会社 シニアマネージャー

山田 素久
PwCコンサルティング合同会社 シニアマネージャー

渕 遼亮
PwCコンサルティング合同会社 マネージャー

松原 翔太
PwCコンサルティング合同会社 マネージャー

www.pwc.com/jp

発刊年月：2021年1月　　管理番号：I202010-07