佐藤 功陛

パートナー
サイバー インテリジェンス センター長

セキュリティ対策で企業価値を守る

サイバー インテリジェンス センター（CIC）は、セキュリティ監視とインテリジェンスの最前線拠点です。インテリジェンスという言葉にはなじみがない方も多いかもしれませんが、サイバー攻撃に対する事前対策を講じるために、国内外のセキュリティ脅威がどのように発生しているか情報収集・分析し、クライアントに情報提供・アドバイザリーを行うことを指します。私たちCICは現在、世界20カ国以上に拠点を構え、グローバル規模のセキュリティ監視とインテリジェンスサービスを24時間・365日体制で提供しています。

日本でCICが設立されたのは2016年。当時はクライアントである日系企業の多くが、セキュリティ監視とインテリジェンスの重要性は一定理解しつつも、セキュリティの脅威が経営リスクに直結するという認識はまだ甘かったように思います。しかし、近年はランサムウェアを使ったサイバー攻撃が急増しました。システムに侵入され、高額の身代金を要求されるというのはわかりやすい一例でしょう。

日本でも多くの企業・団体がランサムウェアの被害を受け、中にはシステムの再構築を余儀なくされ、数カ月も事業運営が滞ったり、決算発表を延期せざるを得なかったりしたケースもあります。結果的に社会からの信頼や評判を損ない、企業価値の毀損につながってしまいます。

しかも攻撃側は、一部の有名企業やグローバル企業に狙いを定めているわけではなく、システムの脆弱性を自動的に検知するツールを開発して、外部から侵入できそうな機器を見つけたら一斉に攻撃を仕掛けます。狙われる先に規模の大小は関係ありません。すべての企業が標的になる可能性があるわけです。そのリスクが広く知られるようになり、ここ数年でクライアントの危機意識は一気に高まりました。

防御だけでなく事前対策を可能にする、DTCYならでの強固なサービス

CICの最大の特長は、セキュリティ監視とインテリジェンスを統合的なサービスとして提供できる点です。国内においてこの2つのサービスを統合的に提供できる企業は他に類を見ません。

CICが提供するセキュリティ監視サービスの特長について説明します。セキュリティ監視サービスは2000年頃から存在していて目新しいサービスではありません。当時の発想は、インターネットの境界を防御して外部からの侵入を防ごうというもので、出入り口を監視することが対策の中心でした。今でも多くの企業・組織が出入り口の監視サービスの提供を受けることで「うちはSOCに監視してもらっているから大丈夫」と思っているかもしれません。しかし、もはや境界防御では新たな攻撃に対処しきれなくなっていますし、境界が突破される、もしくは境界が既に突破されていることを前提にして監視を行う必要があります。

実際、警察庁のデータでは、ランサムウェア被害の約8割は、VPN装置やリモートデスクトップなどのいわゆる企業や組織の「表玄関」とは異なるところからの侵入でした。これに対抗するには、侵入されることを前提として、いかに早く脅威を検知し封じ込めるかが重要になります。

CICでは、ダークウェブなど一般にはなかなかアクセスできない領域も含めた国内外の情報源から、クライアントの脅威となるインテリジェンスを収集し、データを分析してレポートを作成。24時間体制の監視を通じて、システム内における不審な挙動をいち早く検知し、速やかに必要な対応を行うなど、予防から一貫してサポートします。事後対応だけでなく、先駆けて施策を打つことでリスクを排除できる。それこそが私たちCICの強みです。

また、サービス全体を通じたフレキシブルな提案体制も大きな強みです。型にはまった一律のサービスメニューを適用するのではなく、できる限りクライアントの事情に寄り添い、最適な形のセキュリティ対策を提供しています。実はCICの設立以来、監視サービスについてはすべてのクライアントに契約を更新していただいています。これもクライアントにとって価値あるサービスを提供している証ではないでしょうか。

それでは、ここで言う変革とはどういうものを指すのでしょうか。われわれデロイト トーマツ サイバー（以下、DTCY）が事業の主軸として注力している〝サイバー空間〟は大きなキーワードになるでしょう。

DTCYはデロイト トーマツ グループに属していた 2 社のサイバーセキュリティ部門の統合により設立された、サイバーセキュリティに特化したコンサルティングファームです。サイバー攻撃や情報流出など、サイバー空間におけるリスクを経営やＤＸ戦略に直結する課題として捉え、新たなサービスやソリューションを提供しています。

デジタル化が加速するアフターコロナにおいては、私たちが普段生活しているフィジカル空間（現実空間）だけでなく、サイバー空間（仮想空間）をいかに活用できるかが重要な点だと考えます。しかしながら、前述のとおりデジタルリテラシーが低く、サイバー空間をうまく活用できていない企業が多いのが実状。だからこそ、顧客に合わせたコンサルティング、いわばサイバー空間をデザインしていくことが、われわれDTCYが残すべきインパクトだと思っています。そこで最近注力しているものの一つとしてご紹介したいのが、スマートシティやスマートワーク、スマートモビリティなど、フィジカル空間とサイバー空間を融合した〝スマートＸ〟です。皆さんも一度は耳にしたことがあるのではないでしょうか。まだ実証実験の段階ですが、東京のある地域でスマートシティを構築するべく、デジタルインフラの整備、そしてサイバー空間を守り、活用していくプロセスの全てにおいて、DTCYが大きく関わっています。

サイバー領域におけるあらゆる知見を吸収できる環境

統合的なセキュリティ監視サービスが求められる領域は、今後さらに広がっていくでしょう。CICが重点領域と定めているのが、IoTや制御系もしくはオペレーショナルテクノロジー（OT）と呼ばれる領域のセキュリティ、そしてV-SOC（Vehicle-Security Operation Center）と呼ばれる自動車領域のセキュリティです。最近ではインターネットと接続したコネクテッドカーが普及し、スマートフォンで鍵を開けたり、リアルタイムで燃費が表示されたり、便利な機能が使えるようになりました。しかし、それは同時にサイバー攻撃の脅威にさらされているということでもあります。CICでは自動車メーカー様に対して、コネクテッドカーとつながっているシステムのセキュリティ監視を手掛けていますが、将来的に自動運転の実用化を視野に入れ、自動車そのもののセキュリティ監視についても議論を進めています。もちろん既存の領域においても、現在の対策をかいくぐる新たな攻撃手法が出てくることは間違いありません。テクノロジーがいかに進化しても、悪意のある攻撃者が存在する限り、いたちごっこはこれからも続いていくでしょう。最後は人間対人間の戦いなのです。

だからこそ、新たなメンバーの活躍に期待しています。先端技術を学び技術者として力をつけたいという方も、クライアントへの貢献度を高めサービス品質を高めたいという方も、そのどちらも活躍できるフィールドの大きさもCICの魅力です。技術そのものの習得もさることながら、磨いたスキルをいかに価値に変えていくか、というマインドのある方であればぜひ新たな一員としてお迎えしたいですね。

キャリアの選択肢の代表例は、海外での活躍です。現在、海外のCICと連携したグローバル案件も増えています。とりわけ、製造業のクライアントなどからは日本でガバナンスをきかせながら、海外工場のマネジメントをしたいというニーズが急増しているのです。こうした展開を見据えて、DTCYではグローバルに活躍できる人材を増やしていくつもりなので、海外のステージで活躍するチャンスはさらに増えていくでしょう。

さらに、サイバーセキュリティの専門家としてのキャリアという意味でもフィールドは広がっています。より高度なシステム監視や、脅威の発見やインテリジェンス情報の収集・分析、そしてサービスの上流から企画・デザインしていくポジションなどきわめて多彩です。サイバーセキュリティの中で、CICで経験できない領域はないと言ってもいいでしょう。
高い専門性を発揮しながら、自身の技術を価値に変換し社会を支えていきたいという思いこそが、私たちの力の源泉です。共感してくれる方と、共に歩んでいきたいですね。

■サイバー インテリジェンス センター（CIC）の紹介については、こちらをご覧下さい

採用ページへ戻る