行政・公共機関編

2023年の予測

セキュリティ、人材、サプライチェーン：
組織のレジリエンスを向上させミッションを
成功に導くためのインサイト

splunk>

先の見えない時代

この数年の政治的混乱、経済の不確実性、サイバー攻撃の激化、そして収束の見えない新型コロナウイルスの世界的パンデミックにより、行政・公共機関のITチームやセキュリティチームの仕事は以前にも増して過酷になっています。特に、ランサムウェア攻撃の増加、サプライチェーンのリスク顕在化など、サイバーセキュリティの脅威が増大しています。さらに人材面では、パンデミック禍で失った要員をいまだ取り戻せずに苦しむ政府機関やNPOに「大退職時代(Great Resignation)」が追い打ちをかけています。

良いニュースは、いくつかの解決策がすでに実行されているか、近く実行される見込みであることです。米国では、2021年5月にバイデン大統領が国家のサイバーセキュリティ向上に関する大統領令14028を発行し、技術近代化基金(Technology Modernization Fund：TMF)が維持されて引き続き資金援助を行っています。また、組織間のコラボレーションが活発になり、自動化やゼロトラストの導入も進んでいます。

Splunkの行政・公共機関担当グループバイスプレジデント兼最高戦略アドバイザーであるJuliana Vidaは次のように話しています。「行政・公共機関はセキュリティの一部自動化を着実に進めています。今後は、巧妙化するサイバー攻撃に対抗するために自動化が活用されると私は予測しています。また、ゼロトラストの正式導入に向けた動きも見られます」

とはいえ、問題解決への道のりは平坦ではありません。行政・公共機関は民間企業に比べて予算も人材も乏しく、責任の重大さゆえに業務に対して保守的になりがちです。

Splunkの行政・公共機関担当業界アドバイザーであるLaLisha Hurtは次のように指摘します。「多くの組織がTMFの存在を知らないか、適切なプロジェクト提案を作成してTMF委員会に提出し承認を得る方法がわからないため、基金を利用していません」

Vidaは、リソースに制約がある環境で効率を向上させるには自動化が効果的であるとして、次のように説明しています。

「行政・公共機関は自動化を取り入れ始めています。組織全体に展開するにはまだあと数年かかりますが、それが実現すれば、繰り返しの多い簡単で事務的な日常業務に時間を費やしている人材を、創造性と革新的思考が求められる付加価値の高い業務に振り分けて、組織に大きな変化をもたらすことができるでしょう」

行政・公共機関には独自の課題が数多くありますが、全体としてミッションが共通しているという利点があります。そのミッションとは「公共の福祉」であり、それゆえに組織間の競争がありません。昨年の予測レポートでは、新たなリスクやサイバーセキュリティ攻撃に対処するために組織が互いに知恵を出し合う中で情報共有とコラボレーションが進むと予測しました。この予測は実現しつつあります。

「この1年で、行政・公共機関と民間企業のパートナーシップが真価を発揮し、大きな効果をあげ始めています」とVidaは言います。「情報共有や連携サイバー防御計画におけるパートナーシップが奏功し、ついにコラボレーションが実現しつつあるのです」

行政・公共機関では変化がすぐに起こることはまずありません。少なくとも、リーダーが望むスピードでは進みません。しかし、適切なツールが登場し、改善機会は目の前に迫っています。

2023年の予測と戦略

予測

人材不足を乗り切るには、長期的な解決策よりも短期的に有効な戦略が求められる

高いスキルを持つ人材は、特に行政・公共機関では確保が困難です。Splunkの**『データイノベーションによる経済効果』業界レポート**では、調査対象となった複数の主要業界で過半数の組織が人材の獲得と維持を重要課題に挙げています。行政・公共機関では、適切なスキルを持つ人材の獲得と維持が一層難しくなっています。Axios社が昨年夏に公開したレポートによると、民間企業がパンデミック禍で失った人材の99%を取り戻したのに対し、**行政・公共機関での回復率は58%**にとどまりました。

自動化は長期的に見れば有望な解決策ですが、Splunkのエキスパートの見方では効果が出るまでに数年はかかります。またuliana Vidaは次のようにも話しています。「自動化の導入が大きな成果をあげたという話は聞いたことがありません。多くの組織はまだ、高度な自動化機能を活かせる段階に達していないのです」

自動化は万能薬にはなりませんが、それでも、早めに計画を立てて既存の投資を活用すれば、目の前の難局を乗り切れる可能性はあります。

Splunkの業界アドバイザーであるTina Carkhuffは、クロストレーニングを取り入れてメンバー間でスキルを共有するチームが増えていると指摘しています。ただし、リスキリングでできることは限られます(また、働きすぎという別の問題につながる可能性もあります)。いずれにしても、**EUでは不足人材が860万人に達する**など、必要なデジタルスキルや技術スキルを持つ人材が圧倒的に足りない状況であり、リスキリングだけで問題を緩和することはできないでしょう。

従業員の定着期間が短いことを想定して、一定の離職率を前提に雇用計画を立てる行政・公共機関も現れ始めています。Carkhuffは次のように説明します。「連邦政府機関、州政府機関、大学は、新卒採用を行っています。こうした若い従業員は通常、給与こそ低いものの、次のステップに進むための有意義なトレーニングや経験を積むことができます。CIOは、これらの従業員が高い給与を求めて離職することを知っています。一方で、離職してキャリアを積んだ従業員がいずれ戻ってきて、より高い役職に就くことも珍しくありません。そのため、官公庁においても一度退職した職員が再び官公庁に戻ってくることを考慮に入れ始めています。」

実際、あるCISOは新卒人材を集めるために大学の近くにSOC (セキュリティオペレーションセンター)施設を設置しました。この人物は官公庁のCISOではありませんでしたが、人材の獲得と維持について官公庁と同じような課題を抱えていました。このCISOは新卒社員を若きアナリストとして育てながら、2年後には好待遇を求めて離職すると想定して人材戦略を立てていました。

行政・公共機関では、既存の投資を最大限に活用することを目的に、ベンダーとのパートナーシップ強化も進むでしょう。

「人材不足に対応するためとはいえ、新しいツールを次々に投入してすべてのプロセスとタスクを自動化するのは難しいでしょう」とVidaは言います。「既存のツールの活用範囲を広げて、1つの果実からより多くの果汁を搾り取る道を選ぶことになると思います」

果汁搾り器を新しく購入する予算がないなら、すでにある道具である「手」を使ってできるだけ効率的に果汁を搾ればよいのです。それはベンダーも望むところでしょう。自社のツールを幅広く活用してもらえれば、顧客維持率が向上するからです。

予測

国による義務化とサプライチェーンリスクへの対応に後押しされて、今後3年以内にSBOM (ソフトウェア部品表)が標準になる

2年前のSolarWinds社製品に対するサプライチェーン攻撃以来、Log4ShellやKaseyaなど、サプライチェーンを狙った攻撃が相次いでいます。組織がこぞってこのリスクへの対応に力を注ぎリソースを投入するのは当然でしょう。実際、Splunkの2022年セキュリティ調査レポートによると、97%の組織が何らかの対策をすでに実施しています。そして今、サプライチェーンのリスクを緩和するための新たな戦略としてSBOMが注目されています。

SBOMは、ソフトウェアパッケージに含まれるすべての要素をまとめたリストです。サプライチェーン攻撃を受けた組織は、製品に含まれる各コンポーネントを調査して、問題のあるソフトウェアをインストールする可能性のあるコンポーネントを特定し、その製品が支えるサービスの利用者に攻撃の影響が及んでいないかどうかを確認する必要があります。

行政・公共機関は先陣を切ってソフトウェアの購入時にSBOMの提供を求めるようになると、Splunkの特別セキュリティストラテジストであるRyan Kovarは考えています。たいていのソフトウェア製品には多くのオープンソースプロジェクトが含まれ、攻撃を受けたときはそれらの提供元を一つずつ確認する必要があります。その中には、Kovarが言うところの「プロジェクト全体がたった1人のノルウェー人によって支えられている」ようなコンポーネントもあるかもしれません。すべてのコンポーネントを特定して、それぞれ攻撃の影響を受けるかどうかを確認するのは骨の折れる作業です。そこでSBOMがあれば、攻撃の影響範囲をすばやく評価できます。

2023年には、サプライチェーンのセキュリティに対する関心が一層高まり、実装が進むでしょう。そして最終的には、行政機関への製品調達にSBOMが必須になると考えられます。「2025年までに、行政機関へのソフトウェア調達でSBOMの提供が義務付けられる」とKovarは予測しています。

行政・公共機関担当業界アドバイザーのLaLisha Hurtは次のように説明します。「一夜ですべてが変わるわけではありません。各機関や調達事務所が徐々にSBOMを求めるようになり、数年後に標準要件になると思います」

しかし、標準化まで待っていては遅すぎます。SolarWinds攻撃やLog4Jに続く新たなサプライチェーン攻撃の危険は目前に迫っています。次に狙われるのはオープンソースの可能性が高いでしょう。なぜならオープンソースの多くは、Kovarによれば「誰も注意を払っていない」状態だからです。

GitHubもその問題を認識し、先手を打って**コード署名のサポート計画を発表**しました。コード署名はデジタル印鑑のようなものであり、オープンソース管理者が作成したコードと、ユーザーがダウンロードするソフトウェアパッケージに含まれるコードが完全に一致していることを検証できます。ただし、このような先制措置を講じても攻撃が止むわけではありません。攻撃を避けられなかったときは、すばやく対応して被害を最小限に抑えられるよう準備しておく必要があります。その手段の1つがSBOMなのです。

予測

プライバシー規制はまず自治体レベルで導入され、その後国レベルで強化される

米国では最近、法規制が改正され、データプライバシーに対する消費者の関心がかつてないほど高まっています。

グローバルセキュリティストラテジストであるMick Baccioによると、昨年くらいからSignalに急に大勢の人が集まり始めています。それまでSignalを利用していたのは自身と一握りの脅威ハンター仲間だけだったとのことです。「それが今では、ベビーブーム世代からZ世代まで誰もかれもがSignalユーザーになっています。これまで一日中オンラインで過ごし、プライバシーについて一切気にしたことがなかった人々が、『自分の発言がFacebookに勝手に記録されているのではないか』と不安になって乗り換えたのでしょう。10年前と比べて意識が大きく変化しているのです」

プライバシー保護に対する消費者の要求の高まりは、何らかのデータを収集する企業(つまり、ほぼすべての企業)に影響を及ぼします。Googleマップやニューヨークタイムズ紙、さらには月経管理アプリやフィットネスアプリに至るまで、企業は消費者のプライバシーを守るためにさまざまな追加対策を講じる必要に迫られるでしょう。

米国では国レベルでもいくつかの動き見られます。プライバシーに対する取り組みは何十年も前から行われてきましたが、昨年夏に議会に提出された米国データプライバシー保護法(American Data Privacy and Protection Act：ADPPA)の草案では、従来よりも踏み込んで、企業が個人から収集できるデータについて国家基準を定め、データの使用方法を規制しています。この法案が可決されるかどうかはまだ不透明です。しかしその前に、州や自治体レベルでプライバシー規制の強化が相次ぐと考えられます。民間企業はこうした地域によって異なる法案に対応する必要に迫られますが、それをクリアできれば、国レベルの最も厳しい規制にも概ね対応できるでしょう。

一方、行政・公共機関にとっては、プライバシーと機密性は昔から常に重大な課題です。新しいデータをさらに大量に収集することで新たな課題が生じる可能性はありますが、考え方を見直すほどの問題ではありません。

Juliana Vidaは次のように指摘します。「市民のプライバシーを守るという考え方は以前からあり、今日も根付いています。それは変わっていません。扱うデータが増えただけです」

これに対して、組織間の情報共有はあまり進んでいません。LaLisha Hurtによると、責任ある情報共有に大きな価値があることは認識されており、セキュリティを踏まえた課題解決に向けて動き出しています。

「情報共有に取り組み始めた当初はためらいもあり、ケーススタディでは特定の状況を細部まで検討していました」とHurtは説明します。「しかし、その後の進捗は順調で、2023年もこの流れは続くでしょう」

予測

ランサムウェア攻撃の職業化が進み、特に幼稚園から高校までの教育機関が格好の標的となる

ランサムウェア攻撃は収まりを見せません。それどころか、ランサムウェア攻撃グループの職業化、組織化が進んでいます。その影響はすでに現れています。4月に公開されたレポートでは、2021年に身代金を支払った組織は46%にのぼり、2020年の32%から増加しています。Splunkのセキュリティ調査レポートでも、ランサムウェア攻撃を受けたことのある組織が79%にのぼることがわかりました。Mick Baccioは次のように説明します。「ランサムウェアはサービス(取り入れやすいもの)からエコノミー (簡単で、収益化するもの)へと拡大したのです。簡単に利用できるため、他のサービスと組み合わせることで、より大きなエコシステムへと進化します。より迅速かつ効率的になるのです。ランサムウェアオペレーターはエンタープライズレベルのIT運用を習得しつつあります」

特にリスクが高まっているのが教育機関です。Splunkの業界アドバイザーであるTina Carkhuffは次のように指摘します。「幼稚園から高校までの教育機関が最もランサムウェア攻撃の標的になっています。ここ最近で大規模なランサムウェア攻撃が数件発生し、CIOはセキュリティ戦略の見直しを迫られています。教育機関のデータ保護戦略の中でランサムウェア対策は最優先課題です」

最優先にすべき理由は明確です。2022年前半に確認された教育・研究機関に対する攻撃は1週間あたり2,297件にのぼり、前年同期比で44%増加しています。しかも、教育機関の被害額は特に高額です。インシデント1件あたりの平均被害額は、一般企業で180万ドルであったのに対して、教育機関では270万ドルにのぼります。この金額には身代金の支払いだけでなく、その他の復旧コストも含まれます。大学はシステムのバックアップを持たないことが多く、ランサムウェア攻撃の被害からの復旧により多くの手間とコストがかかるのです。

とはいえ、希望がまったくないわけではありません。2022年9月、米国CISA (サイバーセキュリティ・社会基盤安全保障庁)は、幼稚園から高校までの教育機関が直面しているサイバー脅威の詳細と、その脅威を緩和するために国と州が行うべきリソース割り当ての推奨策を示した、議会への提出義務のある報告書を発表しました。行政・公共機関がサイバーセキュリティに費やす予算もまた増えているのです。

Carkhuffは次のように指摘します。「25%の組織がサイバーセキュリティ対策のための予算を以前よりも増やしています。同時に、CISOの平均給与も上がっています。教育機関では、委員会レベルでセキュリティへの関心が高まっています。セキュリティツールやセキュリティ人材への投資を増やす余裕のない機関の多くは、代替手段としてサイバー保険への加入を検討するでしょう」

サイバー保険は、財務面での打撃を緩和する点で効果的な改善策になり得ます。基本的なサイバーセキュリティ対策は多くの攻撃に有効ですが、すべてを阻止することは不可能です。

「ランサムウェアは衰える様子がなく、サイバー犯罪はたちが悪くなる一方で、無秩序に拡大するハイブリッド環境はさらに複雑化するでしょう。そしてそれは、組織全体のレジリエンスを脅かします」と、グローバルセキュリティストラテジストのMick Baccioは言います。「サイバーレジリエンスの優劣が組織のレジリエンスの優劣を大きく左右することになるのです」

予測

IT運用とセキュリティの間でツールとデータの統合が進むと、CISOはITレジリエンスという幅広い観点で(徐々に)より多くの責任を担うことになる

IT領域やセキュリティ領域で「レジリエンス(耐障害性および回復力)」という言葉をよく聞くようになりました。ここ数年の状況を考えれば当然と言えるでしょう。私たちは、すべての攻撃、ミス、障害を完全に防ぐことはできないことを学びました。そのため、これらのインシデントをどれだけ最小化できるかだけでなく、これらのインシデントからどれだけ回復できるかも真剣に考える必要があるのです。

「どの組織でもレジリエンスは部分的に達成されています」と、SplunkのEMEA担当チーフテクニカルアドバイザーであるMark Woodsは言います。「多くの組織にとって問題は、その部分的な成果を1つに結び付けてビジネス全体に広げられないことです。そもそも現時点で、レジリエンスが実際に何を意味するのかについて共通認識はありません」

「レジリエンスはサイバーハイジーンと同じ意味で使われることがよくあります」と、Splunkの特別セキュリティストラテジストであるRyan Kovarは言います。「ITインフラ全体のレジリエンスを向上させたい場合、サイバーレジリエンスの向上が中心になるからです」

レジリエンスへの取り組みで先行しているのはEUで、すでに金融など一部の業界を対象に規制が導入されています。米国では法規制の整備が遅れているため、民間企業や行政・公共機関は自主的に戦略を実行する必要があります。先行するEUに続く方法の1つは、レジリエンスの解釈を広げてCISOに指揮を執ってもらうことです。

「通常、高度な監視を適切に行う方法を知っているのは、それが不可欠なセキュリティチームだけです」とWoodsは説明します。「高度な監視なしにセキュリティ業務は成り立ちません。それ以外の業務は監視なしでもできます。それでうまくいくかどうかは別の話ですが」

「私たちは組織全体のレジリエンスについて何十年も前から語っていたのです」と、Splunkのセキュリティ製品担当グループバイスプレジデントであるPatrick Coughlinは言います。

脅威インテリジェンスのスタートアップであるTruStar社を共同創設したCoughlinによると、かつては「サイバーレジリエンスとは何か」と10人に尋ねれば10通りの答えが返ってきたといいます。

「しかし最近、NISTがサイバーレジリエンスの定義についてすばらしい見解を発表しました。それは、インフラ層の障害であろうと、アプリケーションパフォーマンスの問題であろうと、サービスの障害であろうと、内部脅威であろうと、あるいは外部からの攻撃であろうと、これからは『インシデントはインシデント』と捉える時代だというものです」とCoughlinは評します。「ビジネスのレジリエンスが脅かされたときは、その原因が状況の悪化であるか悪質な攻撃であるかに関係なく、問題をすばやく検知し、修正して、次回から自動で対応できるようにプロセスを変更することが重要なのです」

組織内でデータがチームやツールごとにサイロ化されず、すべてのデータを活用できるようになれば、セキュリティチームはリスクに対してより包括的なアプローチをとることができます。

「データ層での統合が組織内の力学とミッションの定義に影響し始めています」とCoughlinは言います。「この変化に合わせて職名や職務内容が変わるとともに、インシデントの定義の拡大を反映してCISOの影響力が組織全体に広がっています。つまり、CISOは以前よりも幅広く意思決定に関わることになります」

行政・公共機関にとってそれは最先端の取り組みです。それでも最終的にはCISOの役割拡大という動きに追随することになるとLaLisha Hurtは考えています。

「CISOの役割は変わっていくでしょうか？もちろんです」とHurtは言います。「ただし、行政・公共機関における進化や変化は民間企業ほど速く進みません。理想を言えば、CISOはCTOやCIOとより密接に連携し、真のパートナーとして共にサイバー攻撃に立ち向かい、重要資産を守っていくべきです。組織に縦割り構造が残る中でこのパートナーシップは絶対に必要です。こうした取り組みも今後数年以内に進むでしょう」

果報は寝て準備して待て

成果は焦っても手に入りません。少なくとも昔の人はそう言いました。これは特に行政・公共機関に当てはまります。行政・公共機関は、社会における重要な任務を担う一方で、民間企業と比べてリソースがかなり限られます。その結果、行政・公共機関についての予測は、セキュリティとIT運用の統合や国家レベルでのSBOM導入を含め、いずれも段階的な進化を予測するものになりました。

最終的には、データの積極活用に投資した組織が真の勝者となるでしょう。「データは新しい形の『力』です」と、Splunkの最高ソーシャルインパクト責任者であるKriss Deiglmeierは言います。「今後5年以内に、政府はデータの力を理解し、データの積極活用に投資するようになるでしょう。成果の向上や効果的な支出と投資に向けたデータ活用の取り組みがボトムアップで進んでいくと思います」

データ活用の取り組みが大きく前進する一方で、目下の任務を遂行するために既存の投資の活用や短期戦略の強化も欠かせません。国レベルの対策を待たず、プライバシー規制の導入は自治体や州が先行し、民間企業を交えた情報共有のための連携も各組織が自主的に行うことになるでしょう。

「官民のパートナーシップは脅威情報の共有につながります」とVidaは期待します。「次のステップは、官民共同でサイバー脅威対策の計画を立て、脅威分析を行い、連携して防御する、コラボレーション体制の構築だと思います」

それは時代の流れです。人材の確保、パートナーシップの構築、データテクノロジーの活用について賢い戦略を立てることが、デジタルテクノロジーをフル活用して今後も優れた公共サービスを提供し続けるために不可欠です。

寄稿者

Mick Baccio

Splunkのグローバルセキュリティストラテジストを務めるMick Baccioは、サイバーセキュリティや脅威インテリジェンスのエキスパートとしていくつかの米国政府機関を渡り歩いた後、SURGeに加わりました。米国大統領選挙で史上初のCISOを務めた経験もあります。趣味は順不同で、脅威ハンティングとエアジョーダンの収集と「サイバー野菜の栽培」(基本的なサイバーハイジーンの徹底)です。

LaLisha Hurt

Splunkの行政・公共機関担当業界アドバイザーを務めるLaLisha Hurtは、IT/セキュリティリーダーとして20年以上の経験を持ち、GDIT社、Capital One社、GE社、FRS (連邦準備制度)を含め、さまざまな民間企業や行政・公共機関でその任務を果たしてきました。

Tina Carkhuff

Splunkの行政・公共機関担当業界アドバイザーを務めるTina Carkhuffは、Splunkに入社する前は、テキサス州ヒューストン市のCIOを務め、Gartner社で幼稚園から高校/大学・研究機関およびヘルスケアを対象としたエグゼクティブプログラムを率いたほか、脳葉酸欠乏症(CFD)研究組織を立ち上げて、自閉症という複雑な問題を抱える家族を支援しています。

Ryan Kovar

特別セキュリティストラテジストを務め、Splunkのブルーチームセキュリティ調査グループ「SURGe」を率いるRyan Kovarは、DARPA (米国国防高等研究計画局)のシニアプリンシパルセキュリティエンジニアなど、セキュリティリサーチャーおよびエンジニアとしての豊富な経歴を持ちます。DARPAについてはもちろん何も語りません。

Patrick Coughlin

SplunkのGTM戦略/スペシャライゼーション担当VPを務めるPatrick Coughlinは、これまでセキュリティに深く関わってきました。サイバーインテリジェンス管理プラットフォームのプロバイダー、TruSTAR社(後にSplunkが買収)では、共同設立者兼CEOを務めました。それ以前にも、米国政府機関や民間企業をクライアントにサイバーセキュリティ / テロ対策分析チームでリーダーを務めています。

Juliana Vida

Splunkの行政・公共機関担当グループバイスプレジデント兼最高戦略アドバイザーを務めるJuliana Vidaは、Splunkに入社する前は、Gartner社でVPを務めたほか、米国海軍で24年間、船やヘリコプターを操縦し、米国防総省で海軍の副CIOを務めました。

Kriss Deiglmeier

Splunkのソーシャルインパクト/Splunk Global Impactの最高責任者を務めるKriss Deiglmeierは、ソーシャルイノベーターとして知られ、世界中の数々のイベントで講演を行っています。最近では『Inside Philanthropy』誌で、米国慈善活動において最も影響力がある女性50人の1人に選ばれました。

Mark Woods

SplunkのEMEA地域担当チーフテクニカルアドバイザーを務めるMark Woodsは、さまざまな組織でエンジニア、コンサルタント、起業家、CTOを務めました。経営陣や国際的な政策立案者にデータドリブンのアプローチが持つ膨大な可能性について説く仕事もしています。

2023年のその他の予測については、IT運用/オブザーバビリティ編、 本編/エマージングテクノロジー編、データセキュリティ編レポートをご覧ください。

詳細はこちら

22-25650-Splunk-Public Sector Predictions 2023-EB-JA-202302