選挙で起こり得る問題

4 年間の調査と実践的な経験から Talos が得た教訓

著者 : Matthew Olney | ディレクター (Threat Intelligence and Interdiction)

Talos
シスコ セキュリティ リサーチ

選挙で起こり得る問題

4 年間の調査と実践的な経験から Talos が得た教訓

Talos
シスコ セキュリティ リサーチ

目次

選挙で起こり得る問題

4 年間の調査と実践的な経験から Talos が得た教訓

Talos
シスコ セキュリティ リサーチ

はじめに

2016 年 6 月 14 日付のワシントンポスト紙で、米国の二大政党の 1 つである民主党のサーバが侵害され、党内スタッフのチャットが監視されたり、数万通の電子メールやドキュメントが流出した経緯が詳細に報じられた[1] 直後から、Talos は長期戦となる選挙のセキュリティ問題に対する調査を開始しました。多くの研究者と同様、米国の選挙運営についての詳細な情報は持ち合わせていませんでした。話が選挙システムに特化したセキュリティ問題となればなおさらです。早い段階で、選挙運営に実際に携わっている人物からできる限り多くの情報を得る必要があると決断しました。まず初めに行ったのは、米国内のすべての州務長官（または同等の職位の人物）に連絡を取り、聞き取り調査を行うことでした。以来、これまで実施してきた調査で得た情報の中には、共有する価値のある重要な教訓が含まれています。

見知らぬ相手からの聞き取り調査に関心を示す人はほとんどいませんでした。調査を行ったのが 2016 年の総選挙の準備期間中であったことを考えると当然とも言えます。そうした逆境にもかかわらず、数名の専門家からの協力を得ることができました。聞き取り調査後、最終的に、ある州における 2016 年の選挙を観察する機会が得られました。これを端緒に、全米の選挙システムの管理・保護を担当する職員と何時間にも及ぶ話し合いを行い、こうした機会でもなければ訪れることもなかった州議会議事堂に足を踏み入れることになりました。性善説に基づいた法律が結果的に一連の新たな脅威を生み出した経緯について学べた、貴重なチャンスでした。どこにでもいる一般的なアメリカ人がある日突然、国家支援のサイバー攻撃から地域社会を守るという重役を任され、しかもその多くは知識が極めて不足しているという現実を目の当たりにしたのです。

このホワイトペーパーは、選挙のセキュリティに関する現時点での Talos の見解を示すものです。米国の選挙システムを構成する基本的な技術要素、状況を複雑にしている米国の政治理論、2016 年以降の取り組みの現状、そして今なお残る課題について取り上げます。本書は、米国の選挙管理における課題の解決に取り組もうとするセキュリティの専門家のための入門書として発行したものです。

内容は多岐にわたりますが、研究者として見落としてはならないことが 3 つあります。1 つ目は、選挙システムが州や郡ごとに異なるという点です。つまり 1 ヶ所での選挙制度をもって、他の場所の選挙制度を判断することはできないのです。2 つ目は、類似点が多くあるものの、選挙セキュリティと企業セキュリティは「似て非なるもの」である点です。選挙によって米国民は政権を選び、国の未来を決めるのです。最後に、公正な選挙システムの維持だけでなく、その強固な安全性とそれを達成するために必要な投資について国民に伝えることが重要であると私たちは確信しています。

攻撃の目的と守りを固める決断

選挙のセキュリティにおける中心的な論点は、最終的な集計が有権者の意向を正確に反映しているかということです。ところが Talos が外国の攻撃者を調査していく中で、懸念すべき問題はそれだけにとどまらないことが判明しました。つまり、攻撃者の狙いは選挙の結果だけとは限らず、州の選挙管理機関に対して有権者が抱く「信頼」や「信用」も狙う可能性があるのです。

1 https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html

これについては、2019 年 7 月の記事「攻撃者の観点から見た選挙のセキュリティ対策」で詳しく説明しています [2]。攻撃者の重要な地政学的目的は、アメリカ民主主義に対する米国の有権者の信頼を損なうこと、ひいては西側の民主主義に対する世界の信頼を損なうことなのです。何らかの問題が発生したという事実だけでも、攻撃者の目的の一部は十分に果たされていると言えます。このことは、地方選挙区から連邦政府、さらには民間に至るまで、関係者全員が自らの決断や言動が攻撃者の目的にどう影響するかについて考慮する必要があることも意味しています。

郡政委員から公職に立候補する政治家に至るまで、選挙に関わるあらゆる人々の決断が、米国の選挙の公正性に対してアメリカ国民と世界が持つ認識に影響するのです。米国の選挙の公正性に疑念を抱かせるようなあらゆる言動は、攻撃者の目的に同調し勝機を与えることにつながるので、慎重になる必要があります。

2016 年の総選挙中にフロリダ州の 2 つの郡で発生した侵害について、FBI は 2019 年 5 月になってようやく同州への説明を行いました。郡は 2016 年にはこの事実を認識していましたが、FBI は当時、州当局には報告しないという決定を下したのです。就任前に行われた選挙について Ron DeSantis 知事は「不正操作などの問題は一切ありませんでしたが、有権者データへのアクセスは可能でした。よくよく考えてみると、有権者データは一般公開されていたのです。データ侵害だと言えばそれはそうです」と、苦しい弁明をしています [3]。選挙で選ばれた理由が攻撃者による選挙妨害ではないと、候補者が後で説明せざるを得ないとすれば、たとえそれが事実であったとしても、攻撃者の勝利なのです。

攻撃者の目的を理解した上で議論に乗せておきたい点は、2016 年にフロリダ州の投票システムに影響を及ぼす外国の攻撃活動について同州政府に報告しないという決断が下されたことにより、困難な状況が生まれてしまったということです。言うまでもなく、当時の FBI の決断は、フロリダ州の選挙セキュリティを固めるうえで州政府が担うべき重要な役割を州から奪ってしまっています。しかし決定的な問題点は、攻撃者に勝利を許してしまったことです。フロリダ州の投票インフラの特定部分へのアクセスを許したばかりか、選挙プロセスを保護するという点で (少なくともフロリダ州にとっては) 連邦政府が信頼できる相手ではないというストーリーが作り上げられてしまい、事態を悪化させました。そして何年も経った後に、当局の責任者が当時の選挙の公正性について弁明する事態に至ったこと、これは明らかに問題だと言わざるを得ません。

フロリダ州に説明を行わなかったことについて、連邦政府がとった行動が誤りであったと示すための十分な情報はありませんが、2016 年に下された決定によって 2019 年 5 月に外国の攻撃者が勝利を収めたことは明らかです。攻撃者はそれ以上の動きを見せませんでしたが、フロリダ州の安全な選挙実施能力、選挙保護における連邦政府の役割、連邦政府と州政府および州政府と地方自治体の協力関係の実効性、そしてフロリダ州の有権者データの安全性について疑問を投げかける結果となりました。私たちが主張したいのは、2016 年に決定を行う際に、攻撃者の目的と、将来発生し得る損害について考慮すべきだったという点です。

つまり、攻撃者の狙いは選挙の結果だけとは限らず、州の選挙管理機関に対して有権者が抱く「信頼」や「信用」も狙う可能性があるのです。

2 https://gblogs.cisco.com/jp/2019/08/talos-lets-destroy-democracy/

3 https://abcnews.go.com/Politics/voter-databases-florida-counties-hacked-2016-governor/story?id=63052842

2020 年 1 月、地方自治体の選挙システムが侵害された場合には州政府に通知するという方針転換を FBI が発表しました [4]。また、過去の決定は、ハッキング被害者の個人情報を保護するための FBI の方針に基づいて行われたとの説明がなされました。ただし誰が被害を受けたのかは今でも公表されていません。つまり、サイバー攻撃を受けた際に有権者に開示するかどうかは、個々の選挙管理機関が決定することになります。

信頼を守る

政治と選挙に携わるすべての人々には、攻撃者の最大の目的を阻止する上で果たすべき役割があります。投票の不正操作、行政の失策、検閲、党派的偏向、有権者詐欺について根拠もなく非難するといった自発的なミスは避ける必要があり、そうした行為は批判されるべきです。こうした非難はいずれも米国の有権者の信頼を損ない、攻撃者の利益につながります。

一方で、セキュリティの成果と進歩については積極的に伝えていく必要があります。州政府は、投資、スケジュール、政策について情報を開示し、地方自治体も同様に情報開示に努めなくてはなりません。また、投票の安全性を確保するための日常的な行動について、市民教育を行う必要があります。民主主義の保護のために政府の各部署が連携して取り組んでいるという信頼感を市民が得るためには、市民の積極的な参画を求め、選挙が適切に管理されていると実感してもらうことが必要です。市民は、自由で公平な選挙を確保するために必要な時間、資金、人員、設備面での投資について理解し、またそうした投資が実際に行われていることを認めなければなりません。

最後に、政府はあらゆるレベルで危機管理広報に取り組む必要があります。Talos が州政府関係者と話し合いを持つ際は、会見場で州務長官を取り巻く状況についてよく議論します。まずは、システムとプロセスを強化することで危機の回避を図りますが、問題が発生した場合にどう対応すべきかについての議論にも時間を費やします。何かがうまくいかないときは、誰に何を伝えるかの判断が重要になります。外国の攻撃者とその配下で情報操作を行う人間は常に、発言と行動を捻じ曲げて破綻した民主主義のイメージを広める機会をうかがっています。これに対抗するため、私たちは机上演習を実施し、その中で大規模な選挙システムの一部への侵害が成功した例を中心

政治と選挙に携わるすべての人々には、攻撃者の最大の目的を阻止する上で果たすべき役割があります。

にシナリオを展開しています。またその一環として、情報伝達に重点を置いています。適切な表現を考えることに時間をかけ、十分すぎるほどの透明性を確保するよう常に提言することで、公式発表を捻じ曲げて誤った情報を流そうとする攻撃者の手口に直接対抗しているのです。

システム全体と個々の構成要素

システムの評価を行う際、私たちは 2 つの側面からアプローチすることにしました。まず、有権者の登録から選挙結果の表示に至るまでシステム全体を確認した後、各構成要素の動作をつぶさに確認することにしたのです。セキュリティの問題は両方の観点から見つけることができます。個々の構成要素の役割を理解するには、システム全体の役割を理解する必要があります。また、選挙の一般的な原則に関する知識だけでなく、特定の選挙システムの複雑さや特質を理解するために時間を割くことも重要です。実際の選挙システムは州や自治体ごとにすべて異なるため、常に新鮮な好奇心と技術面に対する深い関心を持ってアプローチする必要があります。このセクションでは、体系的なアプローチについて説明し、米国の選挙におけるベンダーの役割について詳述します。また、今日の選挙システムで一般的に見られる基本的な構成要素の一部について掘り下げます。

4 https://apnews.com/dca69532127c625956be9e8d6e6a5c2b

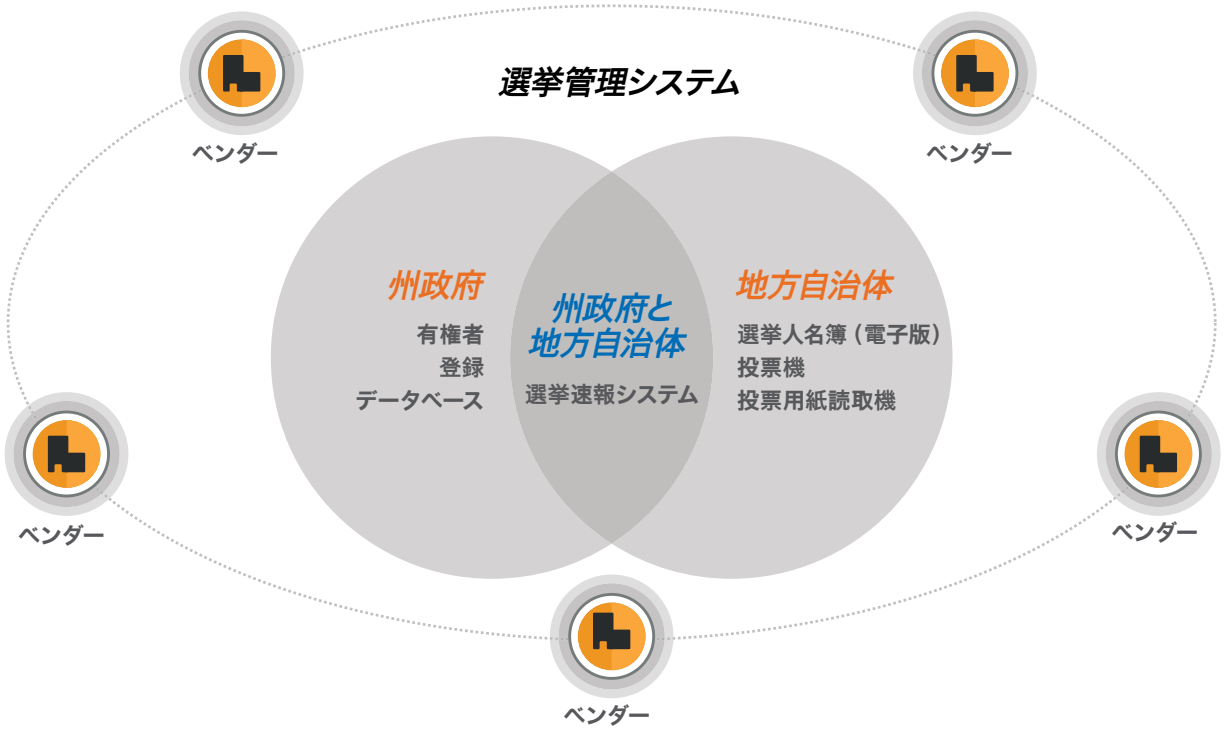

図 1. 主要な選挙技術に関する一般的な責任範囲。
通常は州政府が選挙管理システムの運用を担っていることに注意。

ベンダーの役割

投票技術ベンダーは米国の民主的なプロセスにとって不可欠です。地方自治体は独自のシステム（アイオワ州が採用している電子版選挙人名簿「Precinct Atlas」[5] など）を開発できますが、選挙を可能にするシステムの中核を担っているのはベンダーです。こうしたベンダーと選挙管理人との関係は 10 年以上も遡ることができ、その間に大きな信頼が築かれています。このような関係は尊重すべきですが、同時に報告内容が現実と一致しているかどうか、また、本来求めるべきすべてのことを州政府がベンダーに求めているかを確認する必要があります。

投票技術ベンダーをはじめとするパートナーは選挙のセキュリティを確保する上で不可欠ですが、最終的に安全な選挙を実施する責任は政府にあります。セキュリティの専門家は、選挙システムの極めて重要な要素のうち選挙管理人が把握できていない部分を特定して説明を行い、設計変更指示書や今後の提案依頼書の内容を修正できるようにする必要があります。その目的は、十分なセキュリティ技術を確保すること、選挙管理人がシステムに問題なくアクセスし、システムの詳細を把握できるようにすること、利用者向け機能と行政向け機能の双方を監査できるようにすることです。

ベンダーがクラウドサービスやホステッドサービスを提供している場合には、この点が特に問題になります。こうしたソリューションは完全にベンダー依存であり、選挙管理人には分かりにくい場合があります。セキュリティの監視についての理解が不足しており、ほとんどもしくはまったく報告がなく、システムのセキュリティの検証とテストを実施する能力が限られているためです。

少なくとも契約書には、選挙管理人が拠り所とするシステムや、そうしたシステムの管理担当者に影響を与えるようなセキュリティインシデントの開示をベンダーに求める条項を盛り込む必要がありま

5 https://www.iowacounties.org/programs/iowa-precinct-atlas-consortium/

す。外国政府が支援する攻撃者は、標的とベンダー間の信頼関係を真っ先に悪用します。過去には、選挙ベンダーを狙ったインシデントも発生しています[6]。選挙管理人はインシデントがいつ発生したかを知る必要があります。それがわかれば、使用しているシステムが影響を受けていないか検証することができるからです。

ベンダーは敵対者ではなく、選挙を行う上での重要な構成要素ですが、リスクを負った営利団体であるベンダーの動機や懸念事項は、必ずしも選挙管理人の動機や懸念事項と一致しない場合があります。外部テストの実施やインシデント対応方針の調整といったセキュリティ管理を選挙管理人が検証し、強化する能力を維持するには、管理の詳細を契約書に記載しなければなりません。選挙管理人がベンダーとの契約を更新する際には、セキュリティの専門家が助言を与える必要があります。

システム全体の確認

以降で紹介するどのデバイスも、システムから独立して存在するものではありません。有権者の投票先を判定するプロセスでは、幅広い方針や手順、デバイス、人員といった要素が複雑に連携しているからです。個々のデバイス単位でシステムのセキュリティを確認していくことは、調査を進める上でおそらく最も効果的な方法ですが、一歩離れてシステムの全体的機能を確認することも必要です。

攻撃者には明確な目的があり、必要なだけ時間をかけて選挙システムの特長を調べ上げることによって、目標達成に最も効果的かつ現実的なルートを割り出します。悪用される可能性があるのは技術的な欠陥だけではありません。間違った研修やプロセス、手順、さらには選挙を運営する人間のミスも悪用されるおそれがあります。セキュリティの専門家は必ず、管理が脆弱な箇所や、人為的ミスが発生し得る箇所や、ハードウェアが故障し得る箇所を精査し、問題を確実に発見できる運用体制になっているかを確認する必要があります。

この点については、Kim Zetter 氏[7] による 2019 年 8 月の記事の中で格好の例が示されています。選挙管理人もテクノロジーベンダーも、デバイスのセキュリティは保たれていると言える主な理由として、そうしたデバイスがインターネットに接続されていないという事実を強調することがしばしばあります。記事では、こうした主張がどこまで正しいのかという疑問を投げかけ、実際はそうではなかった事例をいくつか取り上げています。以下は、記事の中で引用されているセキュリティ研究者の Kevin Skoglund 氏の言葉です。

「ある事例では、[ベンダー] が [システムの設置] を担当しましたが、誰もそれを監視していませんでした。選挙管理人は、「自分たちが把握している限り、システムは一度もインターネットに接続されたことはない」と発表していました」

この発言からは 3 つのことがうかがえます。繰り返しになりますが、まず、選挙管理人は投票システムベンダーの言い分が正しいかを監査し、チェックできる立場にある必要があります。次に、Skoglund 氏がリモートでこれを確認できたということは、外国政府の支援を受けた攻撃者にも同じことが可能であることを意味しています。そして、選挙管理人による発表が後になって誤りだと判明したときには必ず、損害がすでに発生しているのです。

セキュリティ専門家の重要な役割の 1 つは、攻撃者の立場から物事を見聞きすることです。きっとこうなるはずと言われていることに注意深く耳を傾け、実際にその通りであることを実験的に検証する必要があります。実際にはそうなっていない場合は、その事実を選挙管理人と共に働く IT スタッフが簡単に判定できるようにする必要があります。常に攻撃者の視点で考え、主張を疑い、プロセスに存在する間隙を探し、個々のシステムだけでなく、そうしたシステムを監視しているシステムの強化も図ることが重要です。

選挙管理システム (EMS)

基本的に、米国の選挙のほとんどは地方で実施されます。選挙は全国の郡や選挙区によって運営されています。ほとんどの州には、州政府と地方自治体の役割を調整する選挙管理システム (EMS) があります。EMS の役割は州によって異なりますが、陪審員候補者の管理、有権者の登録、投票用紙の作成と管理、選挙人名簿の作成と選挙報告などがあります。

通常、EMS は州の専門業者によって特別仕様で作成され、選挙区が有権者データを取り扱うための標準的なメカニズムとして機能します。つまり、EMS はセキュリティ評価を行う上で極めて重要なタッチポイントなのです。EMS の調査は徹底的に行う必要があります。なぜなら、多くの EMS はカスタムコードを使用して設計されていて、地方自治体や州政府が利用するインターフェイスを搭載しているだけでなく、ベンダーが基本システムのトラブルシューティングや管理を行うためのリモートアクセスも可能だからです。

Talos の経験上、評価の範囲を特定する最も手っ取り早い方法は、実践的なデモを見てシステムの使用状況と管理状況を確認することです。なぜなら、こうしたシステムで使用されている用語の定義

6 https://www.rollcall.com/2019/04/22/mueller-report-russia-hacked-state-databases-and-voting-machine-companies/

7 https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

は曖昧であり、カスタムコードが使用されているからです。たとえば私たちが観察したシステムの中には二要素認証機能を備えたものもありましたが、認証方法は、アクセスコードが印字されたビンゴカードを使用するものから、SMS ベースのソリューション、さらには最新の商用多要素認証ソリューションを使用するものまで多岐にわたりました。

EMS は地方自治体が有権者登録データベースを修正する際に使用する最も一般的な手段であるため、攻撃者にとって格好の標的となっています。攻撃者にしてみれば、データベースを直接狙うより EMS を狙う方が目的を簡単に達成できるからです。また、もともとリモートアクセスができるように設定されているため、選挙システムの他の構成要素よりも簡単にアクセスすることが可能なのです。

有権者登録データベース（VRDB）

有権者登録データベース（VRDB）は、有権者に関するあらゆる登録情報を保管する中央データベースです。有権者の最終投票日、陪審員としての活動、それぞれの州が必要とするその他の情報なども追加情報として含まれることがあります。2002 年に制定されたアメリカ投票支援法（HAVA）により義務付けられている VRDB は、有権者登録制度のないノースダコタ州を除き、すべての州が所有するデータベースです。

こうしたシステムの構成要素を評価する際はデータベースセキュリティのベストプラクティスを探る必要がありますが、VRDB に関連するシステム全体に焦点を当てることも重要です。VRDB は一般に選挙管理システムの一部に組み込まれているため、システムとどのように接続されているかを詳細に分析する必要があります。また、他のシステムが VRDB にアクセスする可能性とアクセス方法も調べることが重要です。

たとえば 1993 年制定の全米有権者登録法（通称「Motor Voter」法）では、運転免許証を取得した場所で有権者登録を行うことが認められています。また多くの州には、有罪判決が確定している市民の投票権をはく奪することを規定した重罪リストがあります。州のシステムでは、こうした変更はどのように VRDB に反映されるのでしょうか。有権者が死亡したり州外に転出した場合、システムではどのように処理され、変更は安全に行われているのでしょうか。選挙システムに対する脅威は、州の他のネットワーク要素にも及ぶでしょうか。

他にも、VRDB を確認する際に考慮すべき行動監視機能があります。VoteShield[8] などの企業が採用している新しいアプローチでは、データベース内の変更を調べることができます。こうした行動分析システムは、悪意のある行動を検出するだけでなく、有権者にとっての懸念事項となり得る人的ミスを防止する上でも役立ちます。

過去には VRDB が主な標的となっていましたが、今後もこの流れは続くでしょう[9]。選挙活動を中断させ、投票所での投票を困難にすることを意図する攻撃者にとって、VRDB、さらには選挙管理人が使用する選挙人名簿を不正操作することは効果的なアプローチとなります。不正操作の影響を受けた有権者は通常、臨時投票を行うことができますが、標的と範囲を入念に絞り込んだ不正操作により、特定の有権者層で、投票の混雑や遅延が発生する可能性があります。このような不正操作による影響は、Talos が選挙管理人と話し合いを行う際に確認する標準的なシナリオの 1 つです。

選挙速報システム（ENR）

選挙速報システム（ENR）は、選挙に関心を持つ市民、報道機関、政治家のために開票結果を一元的に提供するシステムです。その方法は一様ではなく、依然として、報道機関が収集した情報を元に各選挙区の開票結果を提示しているだけの州もあります。過去に米国以外の選挙が狙われた事例では、外国政府の支援を受けた攻撃者が偽のデータを流布するために ENR システムを標的にしたことがありました。このことからも、ENR システムへの攻撃は常套手段だということがわかります。

地方自治体によっては、選挙情報の提供に ENR 以外のシステムも使用されています。

Web サイトで開票結果が報じられることもあるため、こうしたサイトも考慮に入れる必要があります。一元管理されている ENR システムとは異なる内容のデータが攻撃者によって地方自治体の Web サイトで公開されると、これまでに説明したような理由から問題が発生する可能性があるからです。公正性への認識に対する影響は、システム自体の公正性と同じくらいに重要です。

また、一部のシステムでは特定の選挙にのみ ENR が導入され、開票結果は地方自治体の選挙用 Web サイトに掲載される例も見られます。これまで Talos は、二重掲載を止め、一元管理されている ENR システムだけを使用するよう推奨してきました。そうすれ

8 https://www.voteshield.us/

9 https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

ば攻撃対象が減り、偽情報を流すことは難しくなります。また、市民が選挙活動の流れを追いやすくなります。

セキュリティの専門家は、選挙区から ENR システムを経てデータが公示されるまでのデータパスを注意深く追跡する必要があります。全体的なプロセスに郡レベルでの検証を含めて、データがシステムに正しく送られていることを確認する必要があります。ENR システムの大部分は、標準的なエンタープライズ情報処理システムとして分析できます。セキュリティの担当者は、こういった対策に加え、プロセスが盤石であり、監査や多要素認証などの適切なセキュリティ管理がプロセスに組み込まれていることを確認する必要があります。また、運用上またはセキュリティ上の問題に対する計画を策定する際には、必ずベンダー、州、郡の間で明確な情報伝達手段を確保し、問題が迅速に処理され情報が適切に行き渡るようにすることが重要です。

選挙人名簿（電子版）

電子版の選挙人名簿（電子選挙人名簿）は、投票所で有権者の受付を行う際に有権者情報を確認するための携帯機器です。電子選挙人名簿を使用すると、有権者登録データベースの適切な部分の写しを容易に入手できるだけでなく、州政府と地方自治体固有のプロセスを選挙人名簿の管理に組み込むこともできます。多くの場合、電子選挙人名簿には、投票所の係員が適切に有権者の受付を行っているかチェックする機能も組み込まれています。電子選挙人名簿にはデータ管理とプロセス管理の両方の機能があり、こうした携帯機器の調達と管理は、州政府ではなく郡政府によって行われるのが一般的です。

種類としてはタブレットやノートパソコン、ID をスキャンするための周辺機器などがあります。実際の運用場面では、有権者の受付情報が複数の機器に反映されるように、1 つの選挙区で使用する複数の機器を接続するためのネットワークコンポーネントが必要となります。評価の際は、個々の機器だけでなくネットワークのセキュリティも確認しなくてはなりません。特に重要なのは、ネットワークアクティビティが投票に必要なものだけに制限されていて、他のアクティビティをすべてブロックする設定になっているかを確認することです。

電子選挙人名簿とネットワークのセキュリティも重要ですが、名簿の保存や設定、データの読み込み方法に関連するプロセスに加え、使用環境も極めて重要です。投票所の係員と選挙管理人向けのガイドラインが書面できちんと整備されていて、選挙管理人の意図が反映されていることを確認しなければなりません。たとえば選挙管理人が無線ネットワークは使用していないと言った場合、システムイメージ、設定、プロセスのすべてにおいて、無線ネットワークが実際に使えないようになっていて、そのことが検証されていることを確認する必要があります。

投票機

HAVA が制定されて以来、現在の投票システムは 20 年前と大きく様変わりしました。投票の処理には、パンチカード式システムや機械レバー式システムの代わりに、コンピュータシステムが使用されるようになりました。この変更は 2000 年の総選挙の結果を受けて導入されたものです。当時、有権者が誰に投票したかが不明だとして 400 ~ 600 万票が無効票となりました。こうした問題がほぼ解消された一方で、投票プロセスにコンピュータシステムが導入されたことにより新たな懸念が生じています。

直接記録電子（DRE）システムでは、有権者がシステムを使って直接投票することができます。インターフェイスはさまざまですが、このシステムの主な懸念事項の 1 つは、投票結果がローカルマシンに記録され、メモリカードや USB に保存された後、中央のシステムでカウントされることです。有権者の投票結果を機械で読み取り、本人が確認できない方法で保存するとすれば、有権者は自分の投票が正しく記録されたことをどのように確認すればよいのでしょうか。

ここでの解決策の 1 つは、DRE に投票確認用監査証跡紙（VVPAT）を印刷するためのプリンタを搭載することです。こうすれば、有権者は投票結果が正しいかどうかを印刷した紙で確認できます。さらに、確認用の投票用紙を使用して再集計と監査を行い、メモリカードに記録されている投票結果をチェックすることもできます。残念ながら最近の調査によると、ほとんどの有権者が印刷した紙の内容をきちんと確認していないことがわかっています。有権者に確認を促す方法や、セキュリティ上のメリットを得るために必要なコンプライアンスの度合いについては、さらに調査を進める必要があります。いずれにせよ、結果を確認できるオプションがあると知るだけでも投票システムに対する有権者の信頼は高まるので、慎重な検討が必要です。

これと同じカテゴリに分類されるもう 1 つのデバイスは、マークシート方式の投票用紙印字機（BMD）です。BMD を使用すれば、有権者が候補者を選択してから投票用紙を印刷できます。集計は別の場所で行われます。BMD は既定の投票システムを使用することが困難な有権者のための支援機器として広く使用されています。

DRE と VVPAT を組み合わせた場合と同様に、BMD を使用する有権者は、自分の投票結果が投票用紙に正しく反映されていることを確認することが重要です。

投票機のセキュリティは長年の研究対象であり、現在でも研究の中心です。たとえ同様のテクノロジーの評価に精通していたとしても、この領域に乗り出そうとするセキュリティの専門家は、この分野にまつわる主要な調査や発言に注目していく必要があります。また、リスク制限監査など、関連する手続きにも詳しくなり、評価対象の投票技術を使用して、そうした仕組みを構築する方法についても理解しなければなりません。

投票用紙読取機

手書きの投票用紙または機械で作成された投票用紙を使用する地方自治体では、投票用紙読取機を使用して投票を迅速に集計し、選挙区レベルで開票結果を開示します。最新の読取機はデジタルスキャン技術を使用しているため、マーキングエラーなどの問題によって手作業で処理しなくてはならない投票用紙を特定できます。通常、読取機はネットワークには接続されておらず、管理された環境にあります。

セキュリティの専門家は、これらのシステムの使用に関するポリシーの管理方法、投票用紙をシステムに送る方法、開票データを収集して上流の機器に送る方法を確認する必要があります。

政治家

政治家の発言や行動は選挙環境において重要な部分を占めます。公職に就いていてもいなくても、アメリカ民主主義に対する有権者の信頼を高めることも損なうこともできる立場にあるからです。このことをはっきりと示すのが、選挙の不正行為の告発です。選挙で不正行為が発生した場合は、徹底的な調査と起訴が必要なことは明らかです。これが選挙の公正性を示すのに役立つ行為であるのは確かですが、根拠のない告発は選挙への信頼を低下させ、権力の平和的な移行を危険にさらします。これでは攻撃者の思うつぼです。

この点でリーダーシップは重要です。州務長官または同等の職位にある事務官は、州で実施する選挙に対する有権者の信頼を高めるための積極的な措置を講じることができる立場にあります。州で実施している対策を積極的に有権者に伝えることが重要な鍵となります。メリーランド州では投票所にポスターを設置し、選挙の安全性を高めるためにどのような対策がとられたかを有権者に示しました。

オハイオ州の情報発信とリーダーシップを事例として紹介します。2019 年 1 月に就任したオハイオ州の Frank LaRose 州務長官は、2019 年 6 月、州内の全 88 郡の選挙管理委員会に対して指令を発し、2020 年の予備選挙に先立ち、郡レベルでの選挙管理のセキュリティを強化するよう求めました。この指令を通じて、州政府は極めて公然とした方法でセキュリティ問題への対応を行っただけでなく、新型コロナウイルス感染症が提示した問題に対するセキュリティ上の変更や調整についても積極的に伝える姿勢をとりました。たとえ決定に反対する声が上がったとしても、枠組みを示し、積極的に情報を発信することが重要なのです。明確かつ正確で広く行き渡るメッセージを発することで、将来起こり得る偽情報キャンペーンに対抗することができます。

選挙管理人は有権者に向けて情報を発信するにあたって、情報伝達手段を標準化し、検証しておかなければなりません。Twitter を使用する場合は、公式アカウントを作成し、Twitter による検証を受ける必要があります。有権者が簡単に情報を見つけられるような、最新の選挙関連ニュースと選挙結果を掲載する公式ページが必要です。有権者に対する教育の一環として、問題の報告や変更の確認、主張の検証を行うための窓口を有権者に周知することも大切です。

政治家をサポートするセキュリティの専門家は、正確な情報が入手可能であることを確認し、状況の把握を妨げる情報の齟齬に対して注意を喚起する必要があります。特に危機の際には、事実に基づいた発言が求められます。現在の調査の進捗状況と、どのような措置が取られているかについて説明することが重要です。インシデント対応計画を作成し、政治家が報道機関の質問に答える際に必要な情報をまとめます。さらに机上演習を行い、質疑応答を試行します。目標は、自由な選挙を妨害する攻撃者に不戦勝を許さないことです。

有権者

民主的なプロセスの参加者として、有権者は自分が手にする情報に積極的に関与する必要があります。今日、情報を健全に保つことは非常に重要です。情報は必ず吟味し、安易に他人と共有しないようにしなければなりません。根拠のない主張は懐疑的な視点をもって判断するようにしましょう。

有権者は、自分たちが偽情報キャンペーンの標的であることを理解する必要があります。有権者の意見や怒り、無関心は国内外の攻撃者に武器として利用されます。有権者は、偽情報拡散のメカニズム、情報処理の心理学、現在の脅威環境において有権者がどのように狙われているのかについて知っておく必要があります。セキュリティの専門家は中立を維持し、偽情報キャンペーンに対処するためのツールと手法を有権者に提供するよう努めなければなりません。

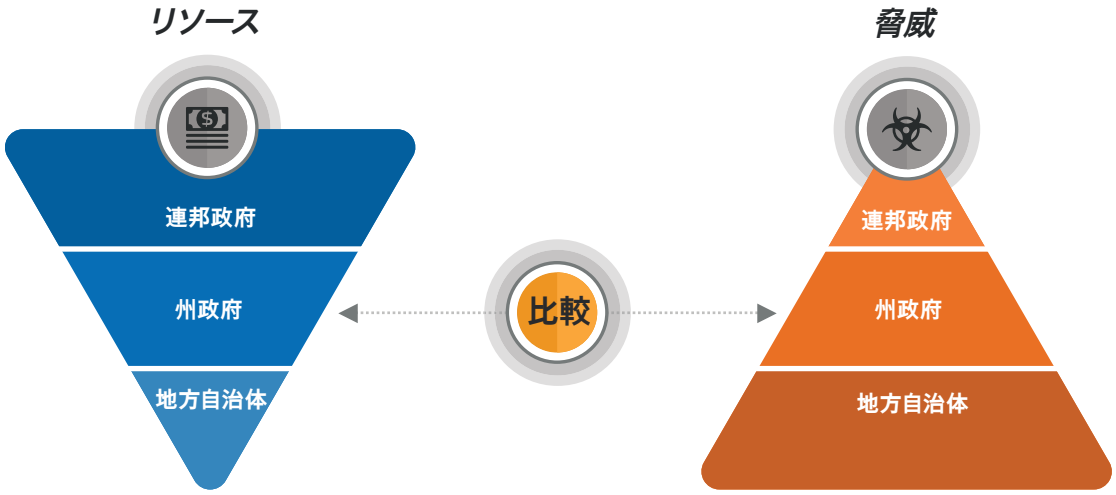

図 2. 連邦政府、州政府、地方自治体が対峙する脅威とリソースの逆ピラミッド関係。

アメリカ民主主義の特異な構造

調査を開始して最初に抱いた感想の 1 つは、選挙システムが州ごとに、また一部の州では郡ごとに異なるため、選挙を完全に乗っ取ることはほぼ不可能だということです。これは確かに楽観的な思考過程ではありますが、米国の選挙はほぼ地方レベルで実施されているという事実に基づいており、これは建国当初から続いている構造なのです。州によって比率は異なりますが、多くの州では、郡がプロセスや実施要項、機器の選択、管理において大きな発言権を持っています。

選挙には、連邦政府、州政府、地方自治体の 3 つのレベルが関わっています。各レベルの政府が、それぞれの立場を尊重する形で事にあたるので、相互に緊張感も見られます。そのことは選挙構造の現実と深く関わっており、危機の際にそれぞれの役割を果たせるよう、全関係者を最適な立場に配置しているのです。

また図 2 に示されるように、3 つのレベルの間で脅威リスクとリソースが逆転しています。選挙の観点から見ると、連邦政府機関を直接攻撃の対象とした場合、攻撃者が得られるメリットは最も少ないでしょう。一方、地方行政を狙えば、極めて大きな成果を上げられる可能性があります。それに対し、連邦政府は、攻撃者の監視と把握を行い、対処する上で遙かに優位な立場にあります。最終的には、この構造の中で最もリソースが乏しい地方行政のインフラが標的となる可能性が一番高いと言えます。

ある州を訪れた際、ヨーロッパの某国出身の専門家が同行しました。その国では選挙に対して中央政府による強力な管理が敷かれています。ある日、選挙の準備にかかる膨大な一連の作業を終え、皆でエレベーターに乗って帰ろうとしていたとき、その

最終的には、この構造の中で最もリソースが乏しい地方行政のインフラが標的となる可能性が一番高いと言えます。

専門家が言いました。「アメリカでは本当にこんなやり方をしているのか?」これらすべてが通常の作業だと説明したところ、ただ首を横に振って「正気とは思えない」と言いました。彼にとって信じがたかったことは、運営面での明らかな欠陥ではなく、選挙インフラをボトムアップで保護することの並外れた困難さだったのです。しかしこれが現実であり、ボトムアップで問題にアプローチする以外に方法はないのです。

州政府と地方自治体

過去 4 年間で私たちは、連邦政府、州政府、地方自治体のそれぞれのリソースを融通し合い、信頼関係を築いて、相互に関与することの重要性を説いてきました。選挙では、州政府と地方自治体の関係が最も重要となります。傾向として、地方自治体よりも州政府の方がインシデント対応のためのリソースに恵まれていて、有利な立場にあります。州政府の立場は地方自治体と似たようなもので、地元の重要人物や制限事項、対応能力についての情報を得て、選挙を実施する上での州レベルでの法的要件を把握することができます。

ここでは問題解決や関係構築と同様に、リーダーシップが重要になってきます。選挙管理の役割と責任を理解し尊重しつつ、それでもなお変化を推進する方法を模索することが非常に重要です。最終的には、州政府と地方自治体の選挙インフラを共通のセキュリティロードマップ上に配置し、連携してインシデント対応にあたり、必要に応じてリソースとサポートを共有し合えるようにする必要があります。これを実現するためには、何年にも及ぶ双方向の忍耐強い協力と、長時間の実践を繰り返していく必要がありますが、外国政府が支援する攻撃を受けて、その対応を郡に委ねることは現実的な選択肢ではないのです。

州政府と地方自治体の交流を評価する際には、まずどのようなサポートパスが確立されているかを確認します。地方自治体の選挙管理人が問題対応時に州に連絡を取る方法や、(状況が許す場合は) 州がどのようにセキュリティ要件を引き下げるかを見ていきます。次に、こうした対応に見られる不備を特定し、サポートパスのあり方を改善する持続可能な方法を模索します。また、問題のある領域を発見するために、州政府と地方自治体双方のリソースを巻き込んだ机上演習の実施も検討します。最終的には、選挙システムに関わる統合インシデント対応計画の確立を目指し、州政府と地方自治体双方のリソースをこの計画に含めます。また、情報伝達とサポートパスに焦点を当てます。

選挙では、州政府と地方自治体の関係が最も重要となります。

地方レベルに関して最後に触れておきたい点は、各郡の間に非常に強固な信頼関係が築かれているということです。多くの場合、郡にとって最も重要なサポートは他の郡から提供されています。たとえばアイオワ州の団体 Iowa Counties Information Technology (ICIT) [10] は、地区内の各郡にリソース共有モデルを提供しています。リソースが足りない郡は、他の郡に専門家の派遣を要請することができます。ICIT によって、もともと存在していた信頼関係とそれぞれの郡の運営体制についての理解が深まったことで、極めてうまく機能しています。こうした対応能力はインシデント対応計画に反映されるべきであり、各州は直接 ICIT に働きかけて、どのような対応を期待できるのかを総合的に理解する必要があります。

連邦政府

行政の観点から見ると、選挙において連邦政府が直接的に担う役割は最も小さいと言えます。連邦政府は選挙管理に関する権限をほとんど持っていませんが、予防的なセキュリティガイダンス、資金援助、情報活動を行っています。これらのサービスの大部分は州が連邦政府へ働きかける形で提供されます。2016 年には物議を醸しましたが [11]、こうした働きかけは 2020 年の総選挙に向けてさらに強まっています。

中でも HAVA による資金援助は最も一般的なものです。最初の数年間は資金援助がありませんでしたが、その後 2018 年には 3 億 8,000 万ドル、2020 年にはさらに 4 億 2,500 万ドルが拠出されました。HAVA による資金援助は不可欠ですが、一部の州当局者は、資金援助に一貫性がないことが大きな困難だと強調して

10 https://iowacountiesit.org/projects/

11 https://thehill.com/policy/cybersecurity/339734-investigation-shows-dhs-did-not-hack-georgia-state-computers

います。ばらつきのある現行プロセスより、額が下がったとしても一定の資金援助を受けられる方が望ましいとまで述べた関係者もいます。

この点は、私たちが初期に話し合いの機会を持った選挙の専門家の意見と合致しています。その人物は、選挙システムの市場経済（連邦政府からの一貫性のない資金援助と州政府と地方自治体レベルでの投資を含む）こそが選挙のセキュリティにおける重要な問題だと強調しました。資金援助に一貫性がないという事実は、ハイエンド企業を欠くことによる市場の機能不全、製品のイノベーションや改善の遅れ、セキュリティインシデントへの対応能力の不確実性につながります。

連邦政府はまた、一貫したセキュリティガイダンスなど、予防的なサービスを提供できる立場にあります。米国国土安全保障省（DHS）傘下のサイバーセキュリティ・インフラセキュリティ庁（CISA）は複数の選挙サービスを提供しています。具体的には、サイバーセキュリティの評価、脅威の検出と防御、情報共有と意識向上、研修とキャリア開発などです[12]。特に重要な要素の 1 つが地域におけるインテリジェンスとセキュリティ分野の専門家の紹介であり、これは州政府と地方自治体の関係構築に役立ちます。Talos では、州レベルと地方レベルの両方で、担当者がこうした専門家の存在を認識し連絡を取り合っているかどうか、常に確認するようにしています。

理論的には州政府は自己資金を調達することができ、セキュリティに関する独自の専門知識も持っています。しかし連邦政府は、タイムリーにインテリジェンスの評価を行って州政府や地方自治体に通知するという点で独自の立場にあります。州政府と地方自治体のリーダーとの話し合いから、この分野での連邦政府の改善が最も期待されていることがわかりました。連邦政府にインテリジェンスと法執行サービスを提供する各種プロバイダーが、現場の担当者に最新のインテリジェンスを提供する役割を担う必要があります。外国政府が支援する攻撃者の動機と行動を理解するために選挙管理人が使用できる選択肢としては、これ以外には考えられません。

4 年間での改善（2016 ～ 2020 年）

2016 年の選挙全般において、アメリカ国民は選挙の公正さを十分に認識できるような行動をとりませんでした。連邦政府と各州の関係は、実効的な協力を可能にするほど強くはありませんでした[13]。そうした状況では、選挙を重要なインフラとして議論することさえ容易ではなかったのです[14]。2010 年連邦会計年度以降、州に HAVA 資金が割り当てられることはありませんでした[15]。州政府や地方自治体に流れてくる情報は非常に少なく、外国からの干渉に対する理解は生まれつつあったものの、それに

2020 年、選挙管理人に新たな課題が浮上

選挙のセキュリティパートナーを最後に訪問して以来、わずか数か月の間に大きな変化がありました。国中がパンデミックに苦しむ中、郵便投票の可能性など、まったく新しい課題が浮上しています。Talos はこれまで郵便投票に取り組んだことはありませんが、他の技術への対応と同様のアプローチを採ることになります。コロラド州、オレゴン州、ワシントン州など、郵便投票システムを長年にわたり問題なく使用してきた州に目を向け、セキュリティの専門家による調査結果を慎重に確認した上で、自身の調査に基づいて行動する必要があります。理解した内容については慎重に発言し、根拠もなく警告を発することを避け、攻撃者が労せずして勝利を手にすることのないように心がけることが重要です。

12 https://www.cisa.gov/election-security

13 https://www.cyberscoop.com/state-election-officials-resisted-federal-cybersecurity-assistance-during-2016-election/

14 https://www.politico.com/story/2016/08/election-cyber-security-georgia-227475

15 https://editions.lib.umn.edu/electionacademy/2018/08/27/eac-releases-details-on-states-plans-for-spending-new-380m-in-hava-funds/

対して連邦政府が打てる 政策には限りがありました[16]。万全とは言えないものの、2020 年の選挙では攻撃者は全く状況が違うことに気付くだろうと私たちは確信しています。

多くの変化がすでに起こっています。HAVA による資金援助は 2018 年と 2020 年の総額で 8 億ドルに上り、投資に活用されています。選挙は今や重要なインフラであり、連邦政府レベルでの資金援助が増加し、重要度も増しています。具体的には、CISA は連邦政府による取り組みにおける選挙セキュリティの中心的役割を果たし、フィッシングテストや脆弱性スキャンなどの一般的なサービスを提供しています。選挙当局間の情報調整を目的として、選挙インフラ情報共有分析センター (EI-ISAC) が記録的な早さで立ち上げられ、州政府と地方自治体では Albert 侵入検知システムとフロー分析システムが広く導入されました。

全米州務長官協会や全米州選挙管理者協会のような組織は、連邦政府機関と連携して、協会のメンバーに向けたメッセージの発信と選択肢の提供を橋渡ししています。Belfer Center の Defending Digital Democracy や Brennan Center for Justice などの学術団体は、選挙管理人との共著による分かりやすいセキュリティガイドラインの提供を行っています。何度か手探り状態に陥ったものの、セキュリティコミュニティと選挙コミュニティは現在、より緊密な連携を図っています。専門知識を共有するため、選挙管理人の呼びかけで研究者が招集されており、Defcon Voting Village のような組織も、より安全な選挙に向けて前進する上で重要な協力者として浮上しています。

あまり目立たないものの中にも重要なものがあります。記者たちは選挙のセキュリティに関する専門知識を磨いています。出版社は選挙のセキュリティに関するスクープを報じるために記者を送り込んでいます。州政府と地方自治体の当局者は、サイバーセキュリティの問題と外国の攻撃者の活動について、認識を深めつつあります。CISA の職員は国を横断して信頼と関係を構築し、選挙のセキュリティにおける連邦政府の適切かつ重要な役割を確立しました。重要な情報を、より迅速に現場に提供するための取り組みが行われています (5 ページの FBI の方針転換を参照)。

まとめ

選挙のセキュリティの課題は、システムの個々の構成要素を確認するだけでは解決できません。これまで直面してきた広範な課題に取り組んだとき以上に体系的な分析を行い、複数の機関と協力して対処する必要があります。外国政府が支援する攻撃者に、州や地方自治体が単独で立ち向かうことはできません。また、そうする理由もありません。パートナーシップを活用できる場面は多々ありますが、リーダーシップが重要な意味を持ちます。選挙当局はセキュリティの重要性を明確に示し、米国の選挙の安全性を確保するにとどまらず、有権者の中に選挙の公正さに対する確固とした信頼を築けるよう、関係構築のための行動をとらなければなりません。

サイバーセキュリティ コミュニティはパズルの一片にすぎません。この問題に取り組むことを選択した私たちにも、信頼を構築し、すべての視点を理解して、限られたリソースで最大の成果をあげられるようにするという責任があります。さらに、他の主要なパートナーとの間の橋渡しを担って、悪意のある攻撃者がどういう行動を起こすかについての理解を共有し、連携して課題に取り組んでいるパートナーとともにそうした理解をさらに深めていく必要があります。

インシデント対応計画を立て、机上演習を実施する際、セキュリティコミュニティは純粋に技術的な懸念事項にとどまらず、情報伝達に重点を置くようにする必要があります。最終的に私たちが守るべきものは、選挙のセキュリティ機関に対する有権者の信頼です。そして、インシデント発生前も発生後も、明確で、誠実かつ正確な情報を発信することが信頼を強化するための鍵なのです。この目標を念頭に、実践を重ね、計画を立て、遂行します。

2020 年になり、私たちは 2016 年当時よりも力をつけていますが、今もなお警戒を怠らず、防御力を強化する必要があります。敵は忍耐強く、より大きな成果を求めて手口を変えてきます。地方自治体、州政府、連邦政府が連携し、民間部門と協力して初めて成功を収めることができるのです。

16 https://www.washingtonpost.com/national-security/obama-teams-response-to-russian-election-interference-fell-short-senate-report-says/2020/02/06/93c2fdac-48f2-11ea-9164-d3154ad8a5cd_story.html

Talos
シスコ セキュリティ リサーチ

Talos について

Talos Threat Intelligence Group は、Cisco Security の脅威インテリジェンス組織です。シスコのお客様、製品、サービス、さらには膨大な種類のオープンソースのセキュリティ製品やツールを対象として、優れた保護を提供することに全力で取り組む、精鋭ぞろいのセキュリティ専門家集団です。Talos は世界最高レベルの脅威リサーチチームであり、7 つの主要な領域（コミュニティとオープンソース、検出リサーチ、エンジニアリングと開発、インシデント対応、インテリジェンスと脅威阻止、アウトリーチ、脆弱性調査と発見）を網羅しています。

Talos は脅威発生と同時に検出と関連付けを行い、数分以内に世界中にカバレッジを提供することによって、既知の脅威と新たなサイバーセキュリティ脅威からお客様を保護します。高い知名度には大きな責任が伴います。Talos はオープンソースのセキュリティもサポートしており、インターネット全体に大きなリスクをもたらす脅威を緩和するために阻止活動を行っています。

詳細については、gblogs.cisco.com/jp/author/talosjapan/ をご覧ください。

著者について

Matthew Olney は、シスコの Threat Intelligence and Interdiction のディレクターです。世界中の公的機関や民間部門のパートナーと連携しながらセキュリティ脅威の特定と対応にあたっているグループのリーダーを務めています。同グループでは、お客様向けのインシデント対応サービスを担当するシスコの組織に向けたインテリジェンスサポートの提供と、大規模なセキュリティイベントに対するシスコの対応の管理も行っています。チームには、WannaCry、NotPetya、VPNFilter といった世界規模の脅威イベントへの対応を主導した実績があります。Matthew は過去 13 年間にわたり Sourcefire とシスコにおいて脆弱性の開発、検出ロジックの作成、アプリケーション開発を担当し、最先端のセキュリティ分析エンジンに関する研究で特許を取得しています。