導入事例 CASE STUDY (TRIPWIRE)

アイオワ州

より強固なセキュリティFortra's Tripwire IP360とCritical Security Controls

昨今の脅威の世界は日々変化と進化を続けており、これまで以上に強力なサイバーセキュリティイニシアチブの必要性が叫ばれています。PwC が発表した『2014 US State of Cybercrime Survey』は、「大半の組織のサイバーセキュリティプログラムは、今日のサイバー犯罪者の執拗な戦術と技術的能力に太刀打ちできていない」と訴えています。それならば、どのように対応できるのでしょうか。標準、ルール、規制、ポリシーが多数存在し、実施と順守が求められるなか、どこから手を付ければよいかの判断が難しくなっています。

アイオワ州の最高情報セキュリティ責任者（CISO）、ジェフ・フランクリン氏は、まったく同じ問題を抱えていました。2009年に彼が着任したとき、アイオワ州は主に、多くの州政府に採用されている一般的なリスクアセスメントフレームワークである ISO 27000 シリーズのセキュリティアプローチを重視していました。ISO 27000 はセキュリティを測るには適切な尺度でしたが、アイオワ州の複雑な環境で必要とされるある運用上の重要な側面が欠けていました。アイオワ州は、脆弱性と実際のリスクを特定し、全体のリスクの状況を把握するための、専門的、体系的かつ信頼性の高い方法を求めていました。何かもっと新しいものを導入する必要がありました。

セキュリティにおける運用上のアプローチには問題がないこと判断されました。アイオワ州 Homeland Security and Emergency Management と連携し、アイオワ州は、州のリスク管理フレームワークとして Council on CyberSecurity 発行の「Top 20」Critical Security Controls（CSC）を採用しました。CSC のアセスメントの 1 つであるリスク評価フレームワークは、脅威の管理と脆弱性スキャンの実施後に残ったセキュリティ上のギャップを特定し対処します。

このフレームワークは、州のセキュリティを、現在そして長期に渡って向上させます。情報セキュリティオフィスは、セキュリティ向上を報告できる、即効性のあるセキュリティ改善策を必要としていました。リスク監査では、投資に対して最大のサイバーセキュリティ効果が望めるのは、CSC のControl 4脆弱性管理（VM）であることがわかりました。この情報に基づき、同州は国土安全保障省（DHS）の資金提供を得て、VM 関連のパイロットプロジェクトを開始しました。

CSC の採用 - より運用可能なセキュリティフレームワーク

同州は、フレームワークとして CSC を採用しました。CSC はサイバー攻撃への対応措置として重要な、優先付けされた 20 のコントロールを提供しているためです。これを実施すれば、現実世界で組織が直面しているリスクへの対応を大幅に強化できるようになります。このコントロールは、セキュリティ上のベストプラクティスのみを示すものではなく、対策が適切に行われていることを確認する方法も提供されているという点で、他のリスク管理フレームワークより運用可能性が高いと言えます。

AT-A-GLANCE

組織: アイオワ州

業種: テレビ放送局

導入製品: Fortra's Tripwire® IP360™

ベネフィット

- 州の機関のほとんどで 50% 以上の脆弱性リスクスコアを低減
- 州の 100 以上の組織で VM ソリューション Tripwire® IP360™ を導入
- プロジェクトの VM カバレッジを IP アドレス数 20,000 から 40,000 へ倍増
- インベントリ機能により、州全体のソフトウェアとハードウェアを可視化し、CSC Control 1 と 2 に対応
- 州のセキュリティリスクの状況を把握するため、州の機関全体で共通のリスクスコアとメトリクスを採用

Control 1 - 5 でインシデントの大部分を防止

- **コントロール 1:** 許可された装置と無許可の装置のインベントリ
- **コントロール 2:** 許可されたソフトウェアと無許可のソフトウェアのインベントリ
- **コントロール 3:** モバイル装置、ラップトップ、ワークステーション、およびサーバのハードウェアおよびソフトウェアのためのセキュアな構成
- **コントロール 4:** 継続的な脆弱性診断および改善
- **コントロール 5:** マルウェアの防御

フランクリン氏は次のようにコメントしています「トップ 5 のControlは、組織を直接的に保護します。他のControlの実施と比較した場合、実際の侵入に対する保護のレベルが高いのです。」

Controlはすべて重要ですが、トップ 5 から 1 つのみを選ぶとすれば、Control 4 の脆弱性管理であるとフランクリン氏は考えています。彼のこの意見は、州が Tripwire® IP360™ を使用して VM パイロットプロジェクトを実施した経験に基づいたものです。また、VM の導入によって、Control 1 とControl 2（許可されたソフトウェアと無許可のデバイス/ソフトウェアのインベントリ作成）の両方も達成できたという副産物もありました。

TRIPWIRE IP360 で大成功

アイオワ州は、多くの企業で利用されており、リスク低減に効果を発揮する VM ソリューションとして TRIPWIRE IP360 を使用し、パイロットプロジェクトを開始しました。導入開始後は、既存の脆弱性を特定し修復するために、州のさまざまな組織と協力しました。これにより、脆弱性リスクを州レベルで 50% 以上も低減しました。ある組織では、84% の低減に成功しています。

この企業全体に渡ってのインベントリ管理は、非常に有益です。たとえば、脆弱性 Heartbleed を狙う脅威が出現した場合、OpenSSL の影響を受けるバージョンを実行するシステムのインスタンスを直ちに検出し、修正を行います。以前はこのような対応には長い時間と、手動での膨大な作業が必要でした。

可視性が向上し、アイオワ州全体のセキュリティに関する判断や考え方に変化をもたらしています。たとえば、システム導入に先駆けて、すべてのシステムの脆弱性スキャンを行うようになりました。

さらに、Tripwire IP360 を利用する州、州組織、都市、郡および学校は、共通の言語を使用してリスクに関する情報を共有できます。各組織は、同一のメトリクスを基準とした標準化されたリスクスコアを使用してリスクを測定しています。測定およびスコアリング方法を共有することにより、グループ間で簡単にスコアを比較検討できるようになりました。さらに、サイバーセキュリティ環境の変化への対応に、行動上の変化をもたらしています。

当初は、一部の州組織、郡政府、学校に同ソリューションを導入することを計画していましたが、まもなく導入対象を拡大しました。「Tripwire IP360 製品の評判が良く、プロジェクトも成功したため、導入対象の組織は 100 を超えています。」とフランクリン氏はコメントしています。

「アイオワをはじめとする州は、ポリシーベースのセキュリティ対策から、運用可能な対策へと移行しました。環境の変化とともに、サイバー攻撃はより高度かつ頻繁になっており、もはやポリシーベースの対策では手に負えなくなったためです。必要なのは、継続的なテストと測定可能な結果です。そのため運用可能な対策が求められるのです。CSC は私達のリスク評価に運用可能性をもたらします。私達が CSC を導入したのはそのためです。」

—ジェフ・フランクリン氏
アイオワ州、CISO

脆弱性管理（VM）のパイロットプロジェクトは即座にその価値を証明

2011 年にアイオワ州は、脆弱性管理ソリューションを選択し、導入プロセスを開始しました。プロジェクトの成功には、国土安全保障省（DHS）の資金提供と、アイオワ州の Homeland Security and Emergency Management 局による管理が不可欠でした。この資金提供によって VM プロジェクトの実施が可能となりましたが、情報セキュリティ局が決定したこのプロジェクトは、同州のサイバーセキュリティリスクに非常に大きな影響を与えるものです。脆弱性管理は、攻撃者の侵入の糸口になるシステムの弱点（古いセキュリティパッチ、または標準から外れた設定）を特定します。多くのセキュリティの専門家は、VM のような対策は、セキュリティ上の重大な問題を始めに一掃できるので、効率が良いと考えています。

CSCトップ20 と TRIPWIRE IP360 の採用で得た成果と教訓

この VM プロジェクトと最新のリスク評価をとおして、アイオワ州は、CSCトップ20　の観点からセキュリティプログラム全体を考えることの重要性を学びました。州のセキュリティプログラムでは、各Control領域のアクティビティに対応し、確固としたセキュリティの基礎を築くことを念頭に置く必要があります。特に、上位 5 つのコントロールの要求を満たすことに注力すれば、セキュリティの状況は劇的に向上します。

もちろん、20　すべてのControlに対応することが理想です。しかし、公共組織でも民間セクターでも、時間とリソースに制限があるため、優先順位付けを行うことを余儀なくされます。

どのControlを最初に行うか（たとえば上位 5つのControlのどれから着手するか）を決定する際には、どのControlで最大の改善が実現できるかを考慮してください。アイオワ州は、Control 4 の脆弱性管理から始めることを推奨しています。なぜならば、ハッカーに悪用される可能性のある弱点を即座に検知し、修正できるためです。

同様に、Control 3 のセキュアなコンフィグレーション管理（SCM）は、設定の安全性を確認することでシステムを保護できます。アイオワ州では、次に SCM 関連のプロジェクトを開始し、VM プロジェクト同様の成功を手にすることを期待しています。

FORTRA™

Fortra.com

Fortraについて

Fortra は、他に類を見ないサイバーセキュリティ企業です。私たちはお客様のために、よりシンプルで強力な未来を創造します。当社の信頼できるエキスパートと統合されたスケーラブルソリューションは、世界中の組織にバランスとコントロールをもたらします。私たちはポジティブ・チェンジメーカーであり、サイバーセキュリティの旅路のあらゆる段階において、お客様の味方となります。詳細については、fortra.com をご覧ください。