シスコ セキュリティ ソリューション導入事例

彦根市

「センサーとしてのネットワーク」による セキュリティ対策の強化と運用の効率化を実現

製品 & サービス

- Cisco Network as a Sensor ソリューション
- Cisco Advanced Malware Protection（AMP）

課題

- 庁内ネットワークと外部アクセス環境の統合に伴うセキュリティ強度の向上と担保
- 外部からの脅威、マルウェア感染へのより強固な対策
- 庁内ネットワークの監視、内部セキュリティ対策の強化
- セキュリティ運用の効率化とコスト削減

ソリューション

- 「センサーとしてのネットワーク（Network as a Sensor）」ソリューションでネットワークの監視、不正通信の遮断、感染端末の隔離などを自動化
- 世界一の検知率を持つ Cisco AMP でネットワークおよび端末のマルウェア対策を強化

結果～今後

- 行政サービスの基盤として、セキュリティの強化と効率的な運用を両立

滋賀県の東北部にある彦根市は、国宝の彦根城、国の特別史跡に指定されている彦根城跡をはじめ、遺跡や神社仏閣、仏像、絵画、史跡など数多くの指定文化財を有しています。琵琶湖に面し、豊かな自然に恵まれており、京阪神、中京、北陸の三大経済圏にも近い格好の立地で人の往来が盛んです。充実した市政の実施に加えて観光 PR も積極的で、公式キャラクター「ひこにゃん」の活躍もよく知られています。

外部対策と同様に内部対策もしっかり行いたいと考えています。シスコのソリューションは監視や隔離を自動化でき、セキュリティの向上と運用の効率化を両立できるところを評価しました。

—— 彦根市 情報政策課　山本 恭裕 氏

彦根市は平成 28 年現在、市役所本庁舎の耐震化整備事業を進めており、行政サービスの基盤をより確実なものとすべく取り組んでいます。ICT 基盤についても、これまで別個に構築、運用してきた庁内（行政システム用）ネットワークと、外部（インターネット）アクセス用ネットワークを統合し、管理工数とコストの抑制を図ろうとしています。市職員が利用するコミュニケーション環境も強化し、自治体としてより早く的確な判断をできるようにするとともに、市民への行政サービスの充実と改善を目指しています。

課題

2 つのネットワークの統合にあたって課題となったのがセキュリティの向上と担保でした。彦根市では ICT 基盤の運用に携わる人的規模が小さく、そうした中で業務負荷を抑えつつ、一定以上のセキュリティ レベルを保つにはどうすればよいかが大きな焦点になりました。

情報政策課の山本恭裕氏は次のように話します。

「昨今のマイナンバーに関することや年金関連の事件などを踏まえ、自治体でもしっかりしたセキュリティへの取り組みは欠かせません。我々の場合、運用に携わる人数が少ないので、セキュリティをある程度以上に保ちつつ管理の負担を少なくするには自動化が必要と考えました。

庁内ではコミュニケーション環境も見直しているのですが、その流れで職員が使う端末がこれまでの 180 台ほどから 1,000 台以上へ大幅に増加することになったのも、自動化が必要と考えた背景です。ネットワークを統合するということは多数の端末が外部アクセス可能となり、脅威にさらされる機会も大きく増えます。

彦根市
情報政策課
山本 恭裕 様

彦根市
情報政策課
古川 達也 様

彦根市
情報政策課
上田 貴美 様

2016 年で誕生から 10 周年を迎える公式キャラクター「ひこにゃん」

ですから、もし何か起きた場合に被害が拡大しないように自動的に通信を止めたり、端末を隔離したりすることができればと思ったのです。マルウェア感染への対策も非常に大きなポイントでした。」

入札によるシステム選定で各社からの提案を受けた彦根市は、シスコの「センサーとしてのネットワーク（Network as a Sensor）」ソリューションと Cisco Advanced Malware Protection（AMP）による対策を採用しました。提案の内容がとても優れていて、求めていた要件に最も合致するものだったと山本氏は話します。

「スイッチ配下の L3 ネットワーク全体の動作（ふるまい）を自動監視するので、通常アクセスしていないところにアクセスしている職員がいるといった場合に、自動的に警告を発したり、その情報を取得したりすることができます。セキュリティ運用ではログの管理は重要ですが、人的に余裕がないことも多いので、ある程度ログの解析などをしなくても対応できる自動監視の仕組みは必要でした。外部からの脅威に加えて内部の対策をどうするかが懸念でしたが、シスコの提案はそこが明確に示されていて、我々にも運用できると感じたのです。

当初は自動化がどこまでできるのか、どのような製品があるかがよくわからず不安だったのですが、シスコは 1 社で必要なものをすべて揃えられるとわかり、これも採用の後押しとなりました。」

情報政策課の上田貴美氏は、次のように補足します。

「必要なものを 1 社で全部揃えるとなると、ベンダー ロックを心配する声もあります。ただ、シスコの製品については知識を持っている構築パートナーは非常に多いので安心感はあります。また、複数のベンダー製品を組み合わせるとかえって面倒になり、特定の構築パートナーへの依存度が上がってしまうことがあるので、運用を別のところに任せるといったことがしづらくなります。今回の選定では、そうしたところも考慮しています。」

よりよい行政サービスの提供に向けて 基盤となるネットワークのセキュリティを高めて 効果的な運用を実現したいと考えています。

ソリューション

ネットワーク全体をセキュリティ センサーに

シスコの「センサーとしてのネットワーク（Network as a Sensor）」ソリューションは、Cisco Catalyst シリーズ スイッチと Cisco IOS Flexible NetFlow で生成された詳細なトラフィック情報、Cisco StealthWatch によるリアルタイム監視やアラートなどを組み合わせてネットワーク上の脅威を見える化します。彦根市ではアクセス認証とポリシー制御を行う Cisco Identity Services Engine（ISE）も組み合わせて、さらにセキュリティ強度を高める構成としています。

情報政策課の古川達也氏は次のように話します。

「今後市民の皆様へどのように行政サービスを提供していくかを庁内全体で考えていく際に、セキュリティという地盤を固めることは非常に重要です。マイナンバーについても、どこまでセキュリティ対策を施すべきかという質問は多いですし、自治体によって対応の差があるのも確かでしょう。彦根市は先進的に取り組んでいるということをアピールする上でも、今回シスコ ソリューションを導入するのは大きな意味があると思います。セキュリティの部分だけで見ると従来よりもコストは上がっていますが、ICT 基盤全体ではコスト削減を果たし、ほかの部分のコストや工数を抑えながらセキュリティに注力しているという位置づけです。」

世界一の検知率を誇る Cisco AMP でマルウェア対策

Cisco AMP はマルウェアの検出とブロック、継続的な分析やアラート発行などを実現するマルウェア対策製品です。シスコがクラウド上に持つ世界最大級のセキュリティ基盤とも連携して、攻撃前、攻撃中、攻撃後という一連のサイクル全体で包括的なマルウェア防御を提供し、標的型攻撃や未知の脅威、ゼロデイ攻撃からネットワークと端末を保護します。第三者機関の調査で、その検知率の高さは世界一と評価されています。

センサーとしてのネットワーク（ふるまい検知）

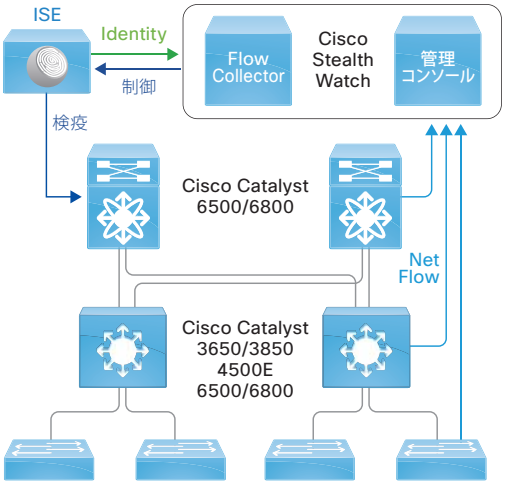
Network as a Sensor

Cisco IOS Flexible NetFlow/Cisco StealthWatch

- クライアント端末の詳細なふるまいを検出
- 異常なトラフィック フローを検出
- ユーザ アクセス ポリシー違反を検出

ポイント

- Flexible NetFlow を利用して、未知の脅威や内部情報漏えいなどの怪しい「ふるまい」を検知 & アラーム送信
- 脅威や外部からの攻撃だけでなく、内部感染や暗号データにも有効
- シグネチャは不要（ふるまいを分析）
- 端末やサーバに対するソフトウェアの追加導入は不要

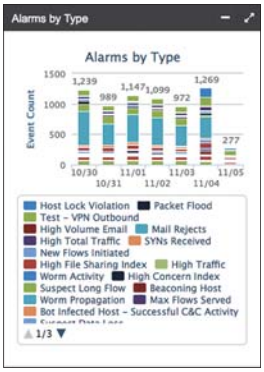


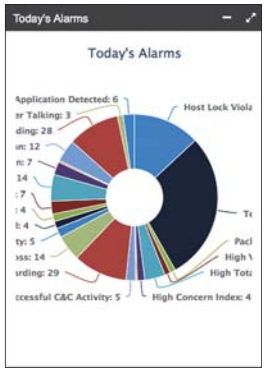
Cisco Catalyst 3650/3850/4500E/6800ia

ネットワーク センサー専用の管理ツール

Cisco StealthWatch

シスコ スイッチ/ルータで収集したトラフィックのふるまい情報から脅威の種類や通信経路、対象端末を自動特定。どの端末で何が起こっているのかを時系列で確認



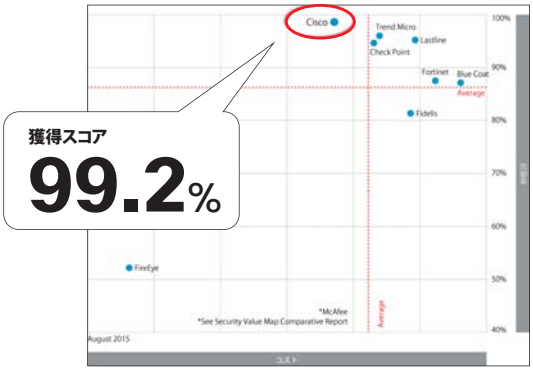


NSS Labs の侵害検知テストで最高スコアを獲得

Cisco AMP

NSS Labs の侵害検知システム（BDS：Breach Detection System）のテストにおいて、最も高いセキュリティ有効性のスコアを獲得

侵害検知システム セキュリティ バリュー マップ



結果～今後

彦根市の新たなネットワーク基盤は構築を進めており、平成 28 年 7 月に第一次構築を終える予定です。その後も市役所本庁舎の耐震化整備事業に合わせて対応し、平成 29 年の構築完了を目指します。新たな ICT 基盤の下で行政サービスを向上させて、生活しやすい街づくり、公共の福祉の増進を実現すべく取り組みを続けます。

その他の詳細情報

Cisco Network as a Sensor ソリューションの詳細は、http://www.cisco.com/web/JP/solution/security/enterprise-network-security/net-sensor.html を参照してください。
Cisco AMP の詳細は、www.cisco.com/jp/go/amp を参照してください。

彦根市

彦根市役所

所在地 滋賀県彦根市元町 4-2

規模 職員数 1,503 名（平成 27 年 4 月現在）
人口 112,728 人（男 55,676 人、女 57,052 人）
世帯数 46,249 世帯
（平成 28 年 7 月時点）

URL http://www.city.hikone.shiga.jp/

彦根市は、昭和 12 年（1937 年）2 月 11 日に市制を施行し、以来びわ湖東北部の中核都市として発展を続けてきました。びわ湖と鈴鹿山系に囲まれた豊かな自然に恵まれた本市は、江戸時代に彦根藩 35 万石の城下町として本格的な歩みを始め、現在に至るまで歴史的、文化的な風情を色濃くとどめるとともに、中世から近世にかけての貴重な歴史遺産が今なお数多く存在しています。

お問い合せ

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

1149-1607-00A-F