\Orchestrating a brighter world NEC

標的型サイバー攻撃対策ソリューション 導入事例

品川区 様

先進的な標的型攻撃対策の導入により多層防御を実現

品川区
企画部
情報推進課長
仁平 悟 氏

品川区
企画部
係長
吉田 義信 氏

事例のポイント

課題背景

- 社会保障・税番号制度の導入にあたり、急増する標的型攻撃から機密情報を守り、情報漏えい防止をより強化し、区政運営の信頼性を向上する必要があった

成　果

- **標的型攻撃を多層で防御**
  インターネット環境を分離し、標的型攻撃を防御する「Application Platform for Secure Web Access」、ファイルの自動暗号化により情報漏えいを防止する「InfoCage FileShell」などを新たに導入
- **低コストで実装**
  先行導入していたSDN※1、およびプライベートクラウドの活用により、設計・構築、および追加機器導入の費用を抑えつつ新たなセキュリティ機能を実装
- **ネットワークとセキュリティを統一的に強化**
  インターネット接続の出入口からエンドポイントの端末までのセキュリティを検討する上で、ネットワークとセキュリティは不可分。より迅速な対応や安全性確保に向け、トータルで任せられるベンダーを選定

(※1) SDN：Software-Defined Networking。ネットワークをソフトウェアで動的に制御すること、およびそのアーキテクチャ。

導入ソリューション

時期	取り組み	内容	製品
2014年10月	サンドボックスの導入	サンドボックス型セキュリティ製品で未知のマルウェアを検知し、ネットワーク内の感染状況を可視化	Deep Discovery Inspector
2015年1月	SDN	全庁ネットワーク基盤の更新	UNIVERGE PFシリーズ
2015年1月	[実証実験] サイバー攻撃自動防御ソリューション	SDNとサンドボックス型セキュリティ製品の連携により動的なネットワーク制御を自動的に行うセキュリティ対策の実証実験	Deep Discovery Inspector、UNIVERGE PFシリーズ、Trend Micro Policy Manager
2015年10月	プライベートクラウド (サーバ仮想化)	全庁仮想化共通基盤の構築	NEC Cloud System (商用製品構築モデル)
2015年11月	個人番号利用事務系ネットワーク分離	SDNによる全庁ネットワーク基盤を活用し、個人番号利用事務系ネットワークを仮想的に新設	UNIVERGE PFシリーズ、FortiGate
2015年11月	総務省「新たな自治体情報セキュリティ対策の抜本的強化に向けて」の発表		
2016年4月	インターネット接続系ネットワーク分離 (インターネット環境分離)	マルウェア感染のリスクがあるインターネット環境と、機密情報を取り扱うイントラネット環境を分離 (SDNを活用しインターネット接続用ネットワークを仮想的に分離)	Application Platform for Secure Web Access、UNIVERGE PFシリーズ
2016年4月	ファイル暗号化	ファイル毎に自動暗号化、自動アクセス制限で第三者閲覧を防御	InfoCage FileShell

お客様名：品川区
所 在 地：品川区広町2-1-36
人　　口：38万2187人 (2016年9月1日現在)
概　　要：「輝く笑顔 住み続けたいまち しながわ」をキャッチフレーズに、安心して住み続けられる安全な街づくりを推進する。JR大崎駅周辺を中心に近代的なオフィス街が広がる一方、歴史や伝統を感じさせる町並みや昔ながらの商店街も数多く残る。防災、教育、福祉サービスの拡充にも継続的に取り組んでいる。
U　R　L：http://www.city.shinagawa.tokyo.jp/

「標的型攻撃への対策を強化するために SDN、サンドボックス、自動暗号化、自動アクセス制限、画面転送など各種技術を活用しています」

品川区 企画部 情報推進課長 仁平悟氏、係長 吉田義信氏に、標的型サイバー攻撃対策ソリューション他をNECから導入した経緯とその効果について詳しく聞きました。

標的型攻撃へのセキュリティ対策の概要

品川区が今回行ったセキュリティ強化プロジェクトの概要を教えてください。

現在、品川区では標的型攻撃を想定したセキュリティ強化を行っています。対策内容は、総務省が平成27年11月に発行したガイドライン、「新たな自治体情報セキュリティ対策の抜本的強化に向けて」に概ね沿っており、今後も順次対応していきます。

ただし総務省のガイドラインが発表される以前から、社会保障・税番号制度の導入を見据えて、本プロジェクトを実施しています。したがって対策内容には、総務省ガイドラインで指定されている施策に加え、品川区が必要だと判断したものに自主的に取り組んでいる内容も含まれます。

施策のコンセプト

今回のセキュリティ強化におけるコンセプトを教えてください。

今回のセキュリティ強化におけるコンセプトは次の3点です。

①標的型攻撃をネットワーク内部に入れないための対策（入口対策）

標的型攻撃とは「特定の組織に対し、悪意を持ってプログラムを送り込むなどして、その組織のネットワーク内部から電子情報を抜き取ることを目的とした挙動」のことです。これを防ぐには、まず悪意のあるプログラム（マルウェア）などをネットワーク内部に入れないという「入口対策」を実施する必要があります。

②情報をネットワーク外部に漏らさないための対策（出口対策）

仮に悪意のあるプログラムがネットワーク内に侵入した場合でも、それと外部との通信を防御することなどにより、重要情報が外部に漏れないようにするための施策、すなわち「出口対策」を的確に実施する必要があります。

③それら対策を的確・迅速・低費用で実施するためのインフラ整備

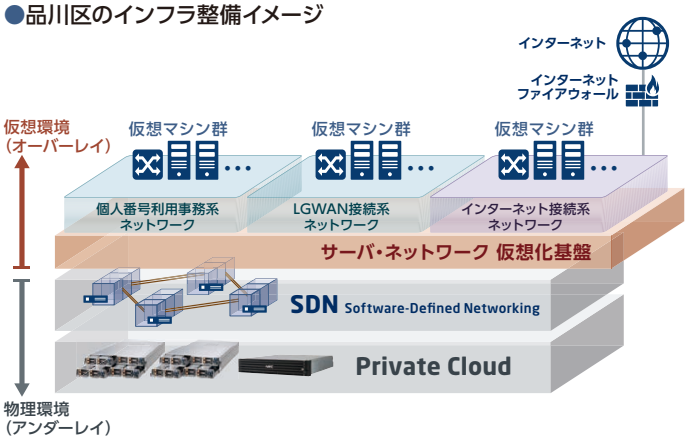
セキュリティ対策は重要ですが、予算には限界がありますし、対策に時間をかけ過ぎてもいけません。必要なセキュリティ対策をその都度、柔軟に、なるべく早期に、低コストで実施するためには、セキュリティ対策のインフラストラクチャ（下部構造）に相当するネットワークやサーバなどシステム基盤を、効率的に管理・運用できる環境を整備しておく必要があります。土台を固めることにより、上物（うわもの）施策の機動性が増します。

施策を、コンセプト別に分類すると次のようになります。

コンセプト	該当施策
入口対策	サンドボックスの導入 個人番号利用事務系ネットワーク分離 メール無害化※2
出口対策	サイバー攻撃自動防御ソリューションの実証実験 インターネット接続系ネットワーク分離（インターネット環境分離） ファイル暗号化 サイバー攻撃自動防御ソリューション※2
インフラ整備	SDN プライベートクラウド（サーバ仮想化）
その他	二要素認証（端末認証強化）※2 共用端末分離（端末セキュリティ強化）※2

（※2）実施予定

●品川区のインフラ整備イメージ



具体的な取り組み内容

取り組み1.「サンドボックスの導入」

**それぞれの取り組みについて個別にお聞きします。
「サンドボックスの導入」とは具体的には。**

未知のマルウェアを侵入させないための「入口対策」です。
標的型攻撃に使用されるマルウェアは何度も使われず、未知のマルウェアであることが多く、ウイルス対策ソフトウェアでの検知は難しいと言われています。そこで、サンドボックス型セキュリティ製品Deep Discovery Inspector（以下DDI）を導入することにしました。
特徴は静的解析だけでなく仮想環境での動的解析によって、静的解析で怪しいと判断されたファイルやプログラムをサンドボックス内で自動実行し、その振る舞いを見て善悪を判断することで脅威を把握します。
これにより、従来の方法では難しい未知のマルウェア検知が可能です。この方法なら標的型攻撃に対しても有効です。

取り組み2.「SDN」

**「SDN」とは。
セキュリティ対策で役立った点を含めて教えてください。**

品川区では2015年に全庁ネットワーク基盤をSDNに更新しました。
SDNとはネットワークをソフトウェアで集中管理する仕組みです。
従来よりもネットワークの増設や変更が容易なので、ネットワーク管理のコストと時間が低減できます。
たとえば従来の方式ではインターネット接続系ネットワークを新設する場合に、新たなスイッチを導入するための期間とコストを要しますが、SDNではそれがほぼ不要になります。
実際、「個人番号利用事務系ネットワーク分離」「インターネット環境分離（インターネット接続系ネットワーク分離）」は、SDNの活用により短期間・低コストで新設できました。
また、SDNは短期間・低コストに加えて「ネットワーク分離の確実性」においても優れています。
VLANなど従来の方式による分離では、ネットワークが設計書どおり実際に分離されていることの担保が難しいと感じました。
ネットワークの可視化ができず、「抜け道が簡単に作れないか」「例外的な経路はないか」「実際には設計意図に反した通信が流れているのではないか」などの確認が困難なためです。
しかしSDNには基本的に分離された論理ネットワーク間の通信をさせない仕組みがあります。
そして、ネットワーク構成、通信のフローに加え、分離された論理ネットワーク状況が可視化されてているため、簡単に確認することができます。
SDNは「厳格なネットワークの分離」を実現する上で最適な仕組みだといえるでしょう。

取り組み3.「サイバー攻撃の即時自動防御の実証試験」

「サイバー攻撃の即時自動防御の実証試験」とは。

マルウェアの動きを封じ込め、情報漏えいをさせないための「出口対策」です。
標的型攻撃に対しては、即時防御が必要だといえます。仮に不審な外部通信をしている端末を検知したとしても、その後の対応が
・ネットワーク管理者にメール通知。その後、管理者が対応する
・サポート部隊がリモートでログインして対応する（あるいは駆けつける）
といった人手による対処では、そこで生じるタイムラグの間にデータ抜き取りなどの攻撃が完了してしまうこと、つまり手遅れになる可能性があります。
そうではなく「不審な外部通信をしている端末を検知した後は、ネットワークが、『ただちに』『自動的に（＝人手を介さず）』遮断する仕組み」を実現したいと考え、サンドボックス等のセンサ装置とSDNを連携させる即時防御の実証実験を2015年1月に行いました。

1. DDIが未知のマルウェアを検知する。
2. DDIは、それをSDN連携アダプタTrend Micro Policy Manager（以下TMPM）に通知する。
3. TMPMは、SDNを制御するUNIVERGE PFシリーズ（コントローラ）にそれを通知する。
4. UNIVERGE PFシリーズのコントローラからスイッチへ、当該端末の通信を遮断するよう指示する。
5. UNIVERGE PFシリーズ（スイッチ）は当該端末のすべての通信を遮断する。

取り組み4.「プライベートクラウド（サーバ仮想化）」

「プライベートクラウド（サーバ仮想化）」とは。セキュリティ対策で役立った点を含めて教えてください。

2015年度には品川区の全庁共通基盤を仮想サーバにより構築しました。
現在は各課の業務サーバを順次移行しています。
このときは、NECからNEC Cloud System（商用製品構築モデル）の提案がありました。
これは共通基盤の構築に必要な仕様、機能をモデル化したものであり、事前検証済みなので、短期間で確実に共通基盤を構築できます。
NEC Cloud Systemには、仮想マシンの新設やリソース追加のための仕様書テンプレートが付属しています。
この仕様書を活用することにより、仮想サーバの経験・ノウハウが少ない品川区でも、スムーズにプライベートクラウドの運用を開始できました。
またこの共通基盤を活用することにより、セキュリティ強化に必要な仮想マシン、あるいは並行稼働用の仮想マシンなどが短期間で新設できました。
従来の基盤では、こうしたマシンの追加・新設は、コスト上の理由により不可能であり、「運用でカバーする」という回避策を採らざるをえませんでした。
共通基盤の活用により、運用で逃げるのではない正攻法のシステム構築が可能になりました。

取り組み5.「個人番号利用事務系ネットワーク分離」

「個人番号利用事務系ネットワーク分離」とは。

マイナンバーなど重要な住民情報を扱うネットワークを、他の業務ネットワークから分離・独立させ、標的型攻撃の侵入経路を防ぎます。
SDNにより、個人番号利用事務系専用のネットワークを短時間かつ低コストで新設することができました。

取り組み6.「インターネット接続系ネットワーク分離（インターネット環境分離）」

「インターネット接続系ネットワーク分離（インターネット環境分離）」とは。

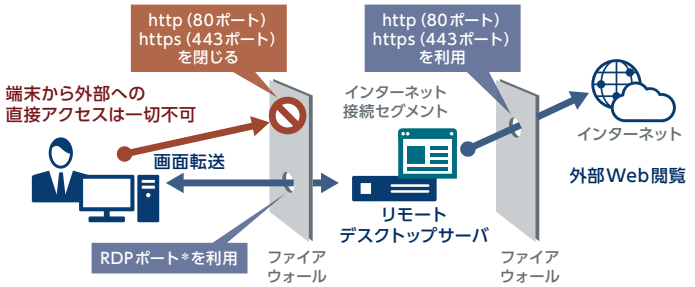
インターネット環境を内部ネットワーク環境から分離し、端末から外部への直接アクセス（通信）を一切不可にすることにより、端末のウイルス感染による情報漏えいを防ぎます。通信を防ぐことによりデータが持ち出されないという意味では「出口対策」といえます。
しかし職員の端末をインターネットから完全遮断すると、検索やインターネット閲覧などができなくなり、業務に支障を来します。
このジレンマは「職員の端末は直接インターネットに接続せず、リモートデスクトップサービスを活用し、画面転送で安全にインターネット閲覧を実現する」Application Platform for Secure Web Accessを導入することで解消しました。
具体的には次のような仕組みです。

1. SDNの機能により、インターネット接続用のネットワークを新設（仮想的に分離）する。その分離したネットワークにリモートデスクトップサーバを設置する。
2. 職員がインターネットを利用したいときには、全てリモートデスクトップサーバを経由させるようにし、業務端末から直接Webサイトを見られないようにする。
3. 職員の端末には画面転送で結果を表示する。
4. これにより、ウイルス感染による情報漏えいを防ぐことができる。
5. 職員の目からは「普通にブラウザを起動してインターネットを利用している」ように見える。特別な操作をする必要はないので利便性は損なわない。

ここで使ったApplication Platform for Secure Web Accessとは NECがこれまで自治体や企業に提供した「ネットワーク分離と画面転送の仕組み」をパッケージ化したものです。すでに安定稼働実績がある仕組みなので、これを使えば要件定義や設計などの作業が大幅に短縮されます。
つまりApplication Platform for Secure Web Accessには要件定義や設計が不要な分だけ、「早く導入できる」「設計および構築にかかる費用が削減できる」というメリットがあります。

Application Platform for Secure Web Access
リモートデスクトップサービス（RDS）を活用したインターネット環境分離

- 端末から直接接続するインターネットアクセスを遮断
- インターネット上のWeb閲覧はリモートデスクトップサーバ上のブラウザ経由で行う
- 業務端末から直接Webサイトを閲覧できないようにすることでウイルス感染を防止



特徴　予め検証済みの統合型システムのため短期間でも安心導入

*RDP：Remote Desktop Protocol

取り組み7.「ファイル暗号化」

「ファイル暗号化」とは。

これは総務省のガイドライン対応ではなく、品川区独自の取り組みです。「万が一、ファイルが外に漏れても、ファイルの中身が閲覧できないため、安全性が向上する」というコンセプトです。具体的な仕組みは次のとおりです。

1. 職員がファイルを保存した場合、InfoCage FileShell（以下FileShell）により自動的に暗号化される。
   - 対象ファイルは「Officeファイル」「PDF」「テキストファイル」「画像データ」「CADデータ」など※3
   - 暗号化は自動的に行われる。職員が手動で操作することはない。

2. さらにその暗号化ファイルには「品川区のネットワークを利用する職員だけが閲覧・編集」できるようにアクセス権がファイル自身に付与される。

3. 万が一、そのファイルが外部に漏えいした場合、ファイルを開いても、ファイルは暗号化されているため、内容を読むことはできない。

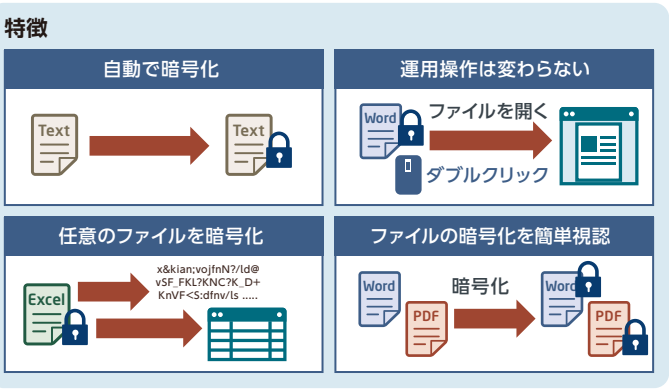
また、FileShellはファイルを自動的に暗号化するので「暗号化忘れ」がなくなります。従来は利用者の判断でファイルにパスワードをつけて管理していましたが、FileShellを導入したことで、対策の徹底が可能になりました。なお、ファイル暗号化を行っても、利用者の操作性は変わらないのでセキュリティと利便性を両立することができます。

「自動アクセス制限」「自動暗号化」は、基本的には「出口対策」です。しかし「漏らさないようにする」というよりは「漏れたとしても安全」という施策なので、むしろ「ファイルが外部に出た後の対策」といえるかもしれません。

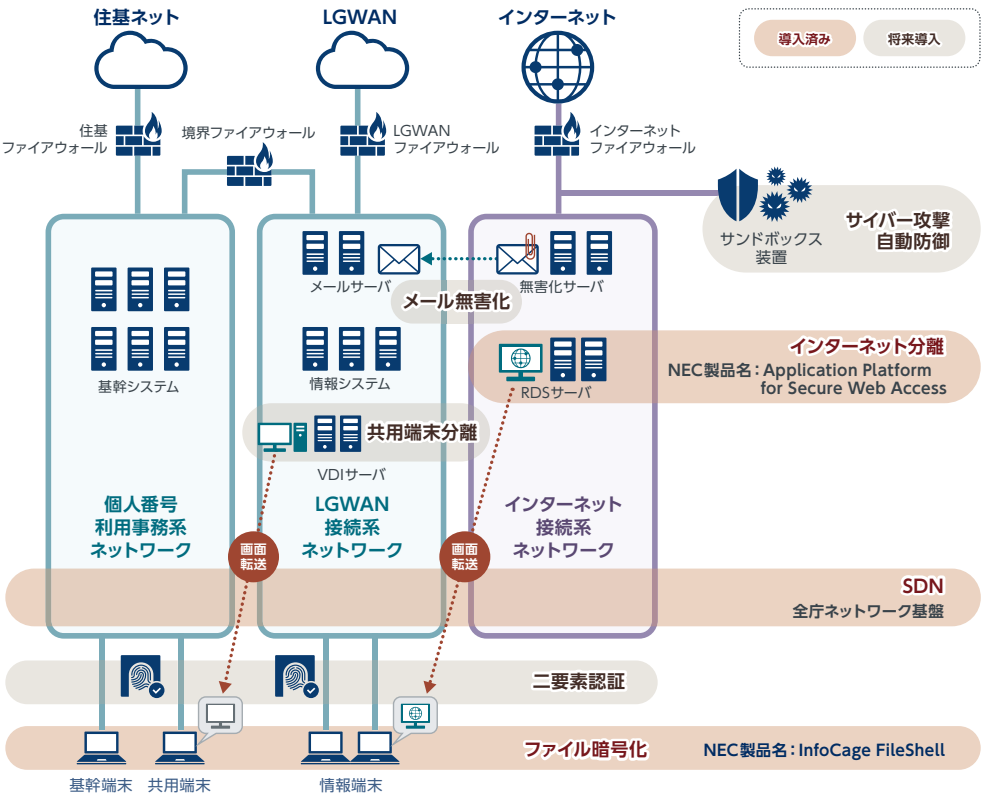
※3 FileShellは、マイクロソフト社のActive Directory Rights Management サービス（AD RMS）を拡張して、Officeファイルだけではなく、PDF、テキスト、画像、CADなどの様々な形式の電子ファイルの保護を可能としている。

InfoCage FileShell
ファイルの自動暗号化を実現する情報漏えい対策ソフトウェア

- 利用者が操作することなく、ファイルを自動暗号化
- 暗号化ファイルは、どこに存在しても、閲覧・編集・コピー時も保護状態を維持します
- 万が一、暗号化ファイルが外部に渡っても、閲覧はできません



●品川区のセキュリティ対策イメージ



なおNECには、これらの標的型攻撃へのセキュリティ対策のほかに基本的なセキュリティ、つまりウイルス対策ソフトウェア、ファイアウォール、IPS（侵入防止システム）、スパム対策などの導入、構築、運用も依頼しています。

今後の取り組み予定（セキュリティ対策の更なる強化）

セキュリティ対策の「今後の取り組み予定」の内容を教えてください。

	取り組み	内容	製品
1	二要素認証	端末へのログイン時、ID・パスワードの他に認証方法を導入しセキュリティ強化	指ハイブリッド認証
2	共用端末分離	デスクトップ仮想化（VDI）活用により、セキュリティを確保しつつ、1台の端末で個人番号利用事務とその他の通常業務を切り替えて行う	VirtualPCCenter
3	メール無害化	インターネットメールの添付ファイルの削除やHTMLメールのテキスト化	※4
4	サイバー攻撃自動防御ソリューション	SDNとの連携により動的なネットワーク制御を自動的に行うセキュリティ対策を全庁へ導入	Deep Discovery Inspector、UNIVERGE PFシリーズ、Trend Micro Policy Manager
5	更なる強化	区政運営における信頼性を向上し、職員負荷を軽減するセキュリティ施策を優先順位を付けて随時実施	

（※4）活用製品は検討中

セキュリティ対策の更なる強化として2016年中に「二要素認証」「共用端末分離」「メール無害化」「サイバー攻撃自動防御ソリューションの導入」を実施していきます。各取り組みの内容は次のとおりです。

今後の予定1. 二要素認証

総務省のガイドラインでは、端末にログインするとき、「パスワードだけ」「指紋認証だけ」のような1要素ではなく、「パスワードと指紋」「指紋とICカード」のように二要素で認証することを求めています。品川区でも適切な形で二要素認証を導入していきます。

今後の予定2. 共用端末分離

共用端末とは、「一台のパソコンでマイナンバーなど重要情報を扱う業務（個人番号利用事務）とその他の通常業務（個人番号関係事務）の両方行う」という端末です。デスクトップ仮想化による画面転送を利用することでセキュリティを確保しつつ、1台の端末で個人番号利用事務とその他の通常業務を切り替えて行います。

今後の予定3. メール無害化

これも総務省のガイドラインでも推奨されている項目です。メールから添付ファイルの削除やHTMLメールはテキスト化などをすることにより、マルウェアの侵入を防ぎます。

今後の予定4. サイバー攻撃自動防御ソリューション

2015年1月に実施した実証実験「SDNとサンドボックス型セキュリティ製品の連携により動的なネットワーク制御を自動的に行うセキュリティ対策（取り組み3）」を全庁へ導入していきます。

また、サイバー攻撃への対策を中心に情報セキュリティには終わりというものはありません。区政運営における信頼性を向上し、職員負荷を軽減するためのセキュリティ施策は、優先順位を付けて適切なタイミングにて実施していきます。

標的型攻撃への対策強化の意義

今回の「標的型攻撃への対策強化」の意義を教えてください。

現在、「悪意ある標的型攻撃」が各所で起きており、自治体も標的とされています。マイナンバーをはじめ住民情報を保有する区として、この標的型攻撃への対策は不可欠だと判断しました。

そのため平成27年度の途中に補正予算を組んで、標的型攻撃への対策強化を決めた次第です。なお一連のセキュリティ施策はバラバラに発注するのではなく、「単一のIT企業に一括依頼し、トータルで安全性を確保する」という方針をとりました。

セキュリティを単一ベンダーに一括依頼している理由

そうした方針をとったのはなぜですか。

第一に「セキュリティの全体整合性を確保したい」と考えたことがあります。部分をバラバラに強化するのではなく、ネットワーク「全体」のセキュリティを整合性ある形で設計し、セキュリティを高める必要があると考えました。
第二に「ベンダー間の調整を極力無くしたい」と考えました。複数の企業にセキュリティ対策を個別に担当させた場合、何か問題が起きたとき、どちらの企業も「ここまでは分かりますが、これ以上は範囲外なので分かりません」となり問題の解決が長期化する可能性があります。この時間を短縮し、よりセキュリティを強化したいと考えました。
第三に「ネットワークとセキュリティを統一的に構築・管理したい」と考えました。外部からの攻撃、内部からの情報漏えい、どちらもその経路はネットワークです。つまりネットワークとセキュリティは不可分であり、この2つは統一的に構築・管理するべきだと考え、インターネットとつながるところから末端までをトータルで任せられるベンダーを探しました。

NECのソリューションへの評価

ここまでのNECへの評価をお聞かせください。

NECの提案に対しては、「品川区が求めるセキュリティ要件を満たしていたこと」「それを早く低コストで実装したこと」を高く評価しています。
コスト削減の最大の要因は、SDNやApplication Platform for Secure Web Accessにより設計・構築費用や追加機器コストを大幅に低減できたことだと考えています。具体的には次のとおりです。

- SDNを使えばネットワーク変更がGUI上で簡単にできる。ネットワーク分離でも、物理的なネットワークの変更は発生しなかった。その分だけ設計・構築費用、そして追加ハードウェア費用が低減できた。

- Application Platform for Secure Web Accessなど「設計構築済みのパッケージソリューション」を使ったので、要件定義や設計の工程が不要だった。その分、設計費用が低減できた。

プロジェクト費用では人件費が大きな割合を占めます。これを合理的に低減できたことで、全体コストを大きく削減できたと考えています。NECによれば、機器費用も含めると、同等規模の自治体で調達しているインターネット分離システムやファイル暗号化システムと比べて、コストは最大6割程度の削減、構築期間は最大4割程度の短縮になるとのことでした。

先行ユーザとしてのアドバイス

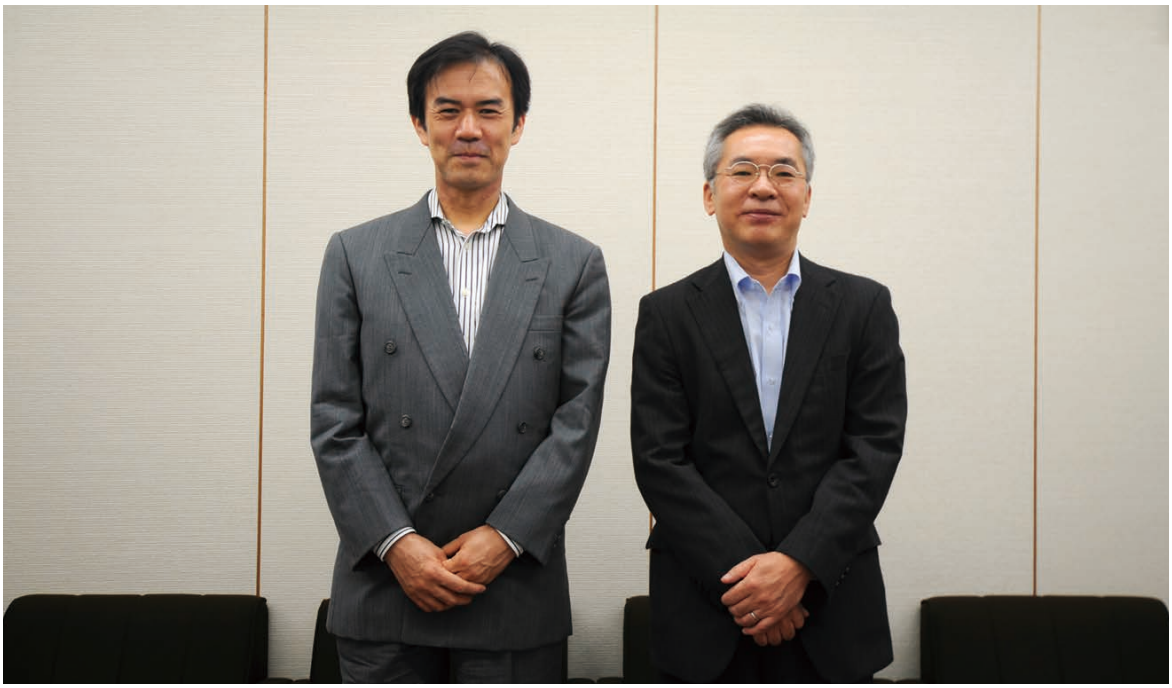
現在、標的型攻撃への対策強化を検討している自治体、団体、企業に向けて、「先行ユーザとしてのアドバイス」があればお聞かせください。

今回は「セキュリティ強化に先立ちSDNを導入したこと」が非常に有効でした。
ネットワークは、セキュリティの「基盤」です。この基盤の柔軟性を高め、変更コストを低減したことで、その上で行うセキュリティ対策を堅牢かつダイナミックに実施できます。SDNという基盤を先に整えたことが効果的でした。

今後の期待

NECへの今後の期待をお聞かせください。

品川区は、効果的・効率的な区政運営に努め、健全財政を堅持しながら、区民が真に必要とする施策を迅速かつ的確に推進していきます。そうした中でも、区政運営におきまして、その信頼性の確保は重要な要素です。昨今ICT技術は目覚ましく進歩しますが、それと同時にウイルス感染や情報の漏えいなどの危険度も増していくでしょう。
そのため、情報セキュリティにつきましては、区民や区の情報を守るために、継続的に強化していく必要があります。引き続きNECには、この情報セキュリティの継続強化に向け、優れた製品、将来を見据えた提案、強固なサポートをいただくことを期待しています。今後ともよろしくお願いします。



写真左より吉田義信氏、仁平悟氏

お問い合わせは、下記へ
NEC プラットフォームソリューション推進本部
E-mail：contact@pfsl.jp.nec.com

日本電気株式会社 〒108-8001 東京都港区芝五丁目7-1（NEC本社ビル）
2016年9月現在
Cat.No. B01-16090345J