\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

ソニー損害保険株式会社 様

入口・出口・内部の各部分に適切な対策を実施。標的型攻撃対策への多層防御を実現

ソニー損害保険株式会社
システム企画部
企画管理課長
松尾 大史 氏

ソニー損害保険株式会社
技術企画課
主査
渡部 陽 氏

事例のポイント

課題背景

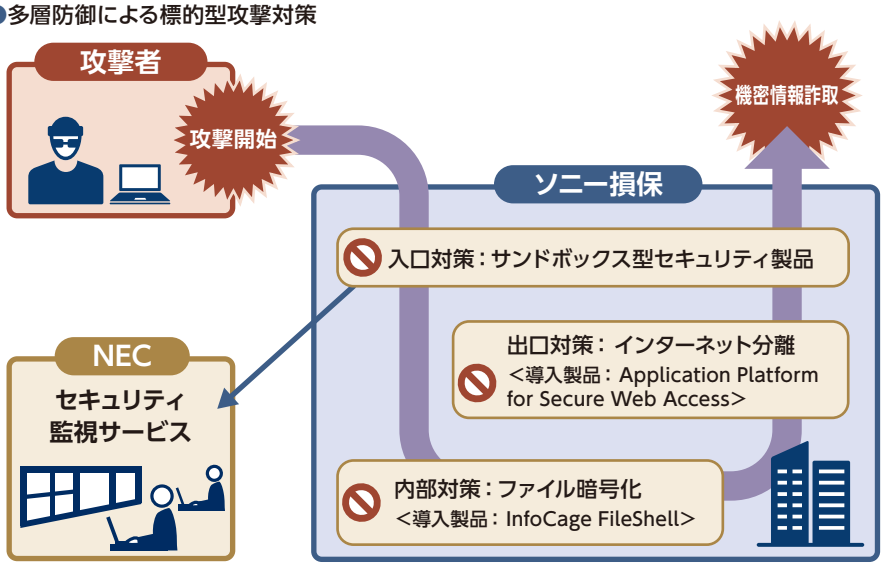
- 内部データの詐取を目的に、特定の企業や団体を狙い撃つ「標的型攻撃」への危機が高まっている
- 「ダイレクト販売の損害保険会社」という業態であり、顧客の個人情報、契約情報が多く蓄積されている。標的型攻撃へのセキュリティ対策強化は急務
- 予算や利便性の維持といった制約の中でも、迅速に実現できる現実的な対策を施す必要があった

成　果

- **セキュリティコンサルティングの有効活用**
  事前にセキュリティコンサルティングを実施。自社の現状を知ると同時に、経営陣に対しセキュリティ投資の必要性を明確に示すことができた
- **標的型攻撃を多層で防御**
  入口対策として、サンドボックス型セキュリティ製品の導入とセキュリティ監視サービスを利用。出口対策として、インターネット分離を実施。内部対策として、ファイルの自動暗号化を実施。正確な現状分析に基づく、メリハリある対策を実現できた

導入ソリューション

●多層防御による標的型攻撃対策



社　　名：ソニー損害保険株式会社
所 在 地：東京都大田区蒲田5-37-1
　　アロマスクエア11F
設　　立：1998年6月10日（ソニーインシュアランスプランニング株式会社として設立）
資 本 金：200億円
事業内容：損害保険業
U　R　L：http://www.sonysonpo.co.jp/

机上の理想論にとらわれすぎないよう、確実かつ迅速に実施できるセキュリティ対策をネットワークの入口・出口・内部に施しました

ソニー損害保険株式会社 システム企画部 企画管理課長 松尾 大史氏、技術企画課 主査 渡部 陽氏に、標的型サイバー攻撃対策ソリューションを導入した経緯とその効果について詳しく聞きました。

ソニー損害保険株式会社について

ソニー損害保険株式会社の概要を教えてください。

ソニー損害保険株式会社（以下、ソニー損保）は、ソニーグループの損害保険会社です。ダイレクト自動車保険では13年連続売上No.1（※1）、保有契約件数163万件超となっています。設立は1998年、年商は955億（正味保険料収入）、従業員数は1119名です（※2）。

※1：自動車保険を主にダイレクト販売している損害保険会社の2014年度までの保険料収入より。ソニー損保調べ
※2：保有契約件数、年商、従業員数ともに2016年3月末時点

標的型攻撃対策のために多層防御を実施

ソニー損保では、今回どのようなセキュリティ対策を実施したのでしょうか。

ソニー損保では、お客様情報の管理・保護体制の向上を目的に、標的型攻撃への多層防御体制を強化しました。
導入した製品、サービスは次のとおりです。

コンセプト	製品・サービス	内容
『入口対策』	サンドボックス型セキュリティ製品、セキュリティ監視サービス	ネットワークの入口にて標的型攻撃の侵入を検知
『出口対策』	インターネット分離 「Application Platform for Secure Web Access」	マルウェア感染のリスクがあるインターネットと、機密情報を取り扱うイントラネット環境を分離
『内部対策』	ファイルの自動暗号化「InfoCage FileShell」	ファイルごとに自動的に暗号化、第三者の閲覧を防ぐ

今回の取り組みの概要は次のとおりです。

項目	内容	備考
施策対象範囲	ソニー損保 本社・支社のネットワーク全体	代理店は除く
施策対象従業員数	約3000名	正規・契約・パート／アルバイトを含む
スケジュール	・2015年8月～：コンサルティング ・2015年10月～：各施策のシステム構築開始、利用者（社内）への説明 ・2016年3月：システム構築完了（※） ・2016年2月～7月：順次、各施策の稼動を開始	※「2015年度内のシステム構築を完了」を目標にプロジェクトを推進し、その目標を達成

十分な効力を持ち、かつ現実的な対策を

今回ソニー損保がネットワークの多層防御に取り組んだ経緯を教えてください。

近年、内部データの詐取を目的に特定の企業や団体を狙い撃つ、いわゆる「標的型攻撃」への危機が高まっており、大手企業、団体で実際に被害にあった事例も報告されています。
ダイレクト販売を中心にした損害保険会社である弊社には、お客様の個人情報、契約情報が多く蓄積されています。標的型攻撃へのセキュリティ対策強化が喫緊の課題であることは、社内の共通認識となっていました。
では、弊社が実施するセキュリティ対策のあるべき姿は何か。私たちシステム企画部では、次のように考えました。

1. 実効性のある、十分な水準の対策であること
自社のセキュリティの現状をよく認識し、防御力が高い、メリハリのある対策を施すべきだと考えました。

2. 制約の中でも実現できる、現実的な施策であること
セキュリティについて机上で理想論を述べるのは難しくありません。しかし、現実には予算や利便性の維持など様々な制約があるため、すべてを理想通りに進めることは困難です。理想を追うあまり、いつまでも対策のメドが立たないのでは本末転倒です。制約を乗り越え、現実に実行可能な施策を策定する必要がありました。

3. 迅速に実現できること
標的型攻撃は、現実に差し迫った危機なので、できるだけ早く対策を取る必要があります。もちろん、不十分な内容の対策を早期に行うような、いわゆる「拙速」では意味もありません。しかし、「時間をかけて最高の対策をじっくり実現していく」という「巧遅」もまた不適切だといえます。

これらあるべき姿の対策を実現するために、社内で協議した結果、まず「セキュリティコンサルティング」を依頼するべきという結論にいたりました。その後、コンサルティングを依頼する企業の選定を開始しました。

セキュリティコンサルティングの依頼先に求めた要件

コンサルティングの依頼先はどのような基準で選んだのでしょうか。

今回セキュリティコンサルティングを依頼する企業は、「コンサルティングへの社内評価が良好である場合、引き続きシステム構築も依頼する」という前提で選びました。依頼先の選定に際し、弊社が求めた要件は次のとおりです。

1. 正確な現状分析ができること
理想論の提示だけでは意味がありません。

2. 分析結果を、経営層に説明できる形で提示できること
技術的専門性に偏らず、経営層に説明可能な形で分析結果をまとめることを求めました。

3. 分析結果に基づき、的確な提案ができること
分析だけで終わらず、具体的な対策案が出せることを求めました。

4. その案の実現・実装まで依頼できること
コンサルティング終了後は、実際のシステム構築も依頼できることを求めました。

5. 総合力があること
特定のセキュリティ分野にのみ強い、というのではなくすべての分野を総合的にカバーできるだけの製品力、ソリューション力があることが必要でした。

6. 大手企業、団体、特に金融機関で十分な実績があること

以上の要件に基づき候補各社を比較検討したところ、NECが弊社の求める要件を最もよく満たしていたので、NECへコンサルティングを依頼することを決めました。

攻撃が本当に来ているかどうかをまず調査

セキュリティコンサルティングはどのように進んだのでしょうか。

セキュリティコンサルティングは次のような順序で進めました。

1. マトリクスで現状を理論的に精査
2. サンドボックス型セキュリティ製品で実際の攻撃状況を調査
3. 攻撃が『実際』にきていることが判明
4. 経営層に説明し、具体的な対策内容を策定

まず、社内のセキュリティ対策の現状を NEC と共にマトリクスを使って精査しました。総合的には「概ね十分な水準」という診断結果となりましたが、「標的型攻撃の脅威を考えた場合、やはり強化した方が良いと思われる点」もいくつかありました。マトリクスは大変便利で、より明確かつ網羅的な分析が可能になり、また結果を一覧表にまとめるのも容易でした。
続いて NEC からは、「まずサンドボックス型セキュリティ製品を一時的に評価導入し、それを使って攻撃が“実際に来ているかどうか”を調べましょう」と提案がありました。調査の結果、攻撃は来ていたものの、マルウェアへの感染は防げていました。
この調査により、「来ているかもしれない」「来ることがあり得る」というのではなく、「(防げてはいるものの) 現実に来ている」ことが、客観的に明らかになりました。
「実際に攻撃が来ている」という調査結果は、経営層をはじめ社内へセキュリティ強化の必要性を訴えるにあたり、説得力の高い情報となりました。セキュリティ脅威が「見える化」できたわけです。
これらコンサルティングの結果に基づき NEC からは、

- 「入口対策」としてサンドボックス型セキュリティ対策とセキュリティ監視サービス
- 「出口対策」としてインターネット分離
- 「内部対策」としてファイルの自動暗号化

が提案されました。

入口対策　～　サンドボックス型セキュリティ対策とセキュリティ監視サービス

「入口対策としての、サンドボックス型セキュリティ対策とセキュリティ監視サービス」とは具体的には。

ネットワークの入口にて標的型攻撃の侵入を検知するための対策です。
標的型攻撃で使われるマルウェアは、特定の対象を攻撃するために作られた専用の悪質プログラムです。これは、定義ファイルを元に検出する従来のマルウェア対策システムでは防げません。
一方、サンドボックス型セキュリティシステムでは、侵入しようとするプログラムの動きを特定のシステム領域（サンドボックス）で調査し、その挙動に応じて悪質か否かを判定するというものです。これなら、標的型攻撃に使われるマルウェアの検知率が高まります。
このサンドボックス型セキュリティシステムには、NEC のセキュリティ監視サービスを利用しています。これは、NEC のセキュリティアナリストが、弊社に代わってサンドボックス型セキュリティシステムによる攻撃検出結果を 24 時間 365 日体制で監視・運用するというものです。これにより、標的型攻撃の迅速な検知と対応が可能になります。

出口対策　～　インターネット分離

「出口対策としてのインターネット分離」とは。

セキュリティ対策を検討するときは、「性善説ではなく性悪説」「楽観論ではなく悲観論を」という前提を取る必要があります。
この場合の「悲観的前提」とは、「いくらサンドボックス型セキュリティ製品で入口対策を実施したとしても、マルウェアがネットワーク内部に侵入する可能性はゼロにはできない」という立場のことです。
多くの場合、攻撃者の目的は、ネットワーク内の重要情報を外部へ持ち出すこと（送信すること）であり、その送信経路としてインターネットが利用されます。ということは、重要情報を格納しているネットワークをインターネットから分離すれば、もしマルウェアが侵入しても、詐取した情報をインターネット経由で外部に送信することはできません。これが、「出口対策としてのインターネット分離」の基本的な考え方です。
とはいえ、インターネットを完全に使用不可能にしたのでは、従業員の日常業務に支障を来します。この問題を解決するために、NEC からは「画面転送によるインターネットアクセス」という提案が出されました。

インターネットの活用を確保しながら、ネットワークを分離するには

「画面転送によるインターネットアクセス」とは具体的には。

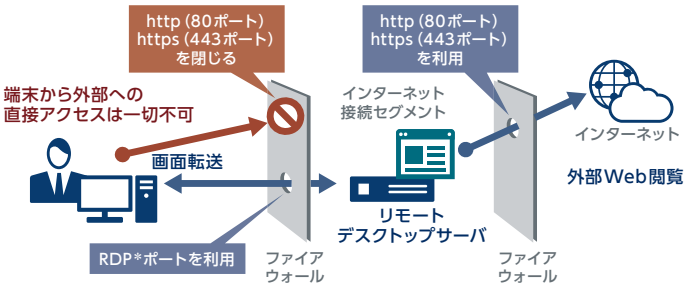
具体的には次のような方法です（インターネット検索を例にして説明します）。

- 従業員の PC はインターネットに接続させない。
- インターネット検索による調べ物などが必要な場合は、「検索結果の画面転送」を使って実現する。
- この場合、インターネットへのアクセスそのものは従業員の PC とは別の隔離領域で行う。従業員の PC にはそのアクセス結果だけを『画面転送』する。

この方式なら、「従業員がインターネットを使うこと」と「従業員の PC をインターネットから分離すること」を両立できます。
なおネットワークが分離されているといっても、職員がネットを利用するときの操作は「普通にブラウザを起動して目的サイトにアクセスする」というものです。従来と同じ操作手順で使えるので、利便性が損なわれることもありません。

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

内部対策　～　ファイルの自動暗号化

「内部対策としての、ファイルの自動暗号化」とは。

これも、インターネット分離と同じく「悲観的前提に基づいた対策」です。ここでの悲観論とは、「どんなに入口対策、出口対策を施しても、社外にファイルが流出する可能性はある」ことを前提にした取り組み姿勢を指します。このファイル流出に対処するために、内部対策として InfoCage FileShell を導入し、「ファイルの自動暗号化」を施しました。具体的には、次のような仕組みです。

- OfficeやPDFなど社内で使う各種業務ファイルがInfoCage FileShellにより、自動的に暗号化されます。

- 暗号化ファイルには「ソニー損保のネットワークを利用する従業員だけが閲覧・編集」できるようにアクセス権限が自動で付与されます。

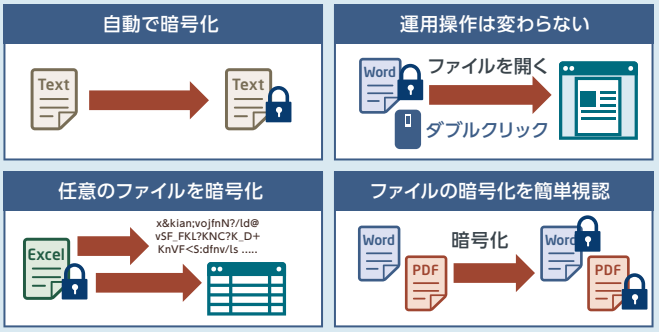
- アクセス権限は、予め設定した権限（編集可能／閲覧のみなど）に基づいて付与され、権限に応じたファイルの取り扱いが可能になります。

これは、「万が一、暗号化されたファイルが社外に持ち出されたとしても、外部の第三者にはファイルの中身が閲覧できない」ことを図った仕組みです。標的型攻撃に限らず、そのほかメール誤送信などの理由によるファイルの社外流出にも対応できます。
また、InfoCage FileShell でファイルを暗号化しても、従業員の操作方法（手順）は従来と変わりません。使い勝手を変えずに、セキュリティレベルを向上させられる点を高く評価しています。

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

特徴



スケジュール遵守を評価

ここまでのNECの仕事への評価をお聞かせください。

今回は、コンサルティングから製品導入、システム構築、運用までをトータルに NECに依頼しましたが、どのフェーズでも期待通りの仕事品質を示していただけました。NECのセキュリティ技術、ネットワークの技術力の高さを再認識しました。
また、要件の一つであった「迅速な構築」が実現されたこと、具体的には「2015年度内にシステム構築が完了したこと」も高く評価しています。
今回のプロジェクトを推進するにあたり、社内には「セキュリティ強化施策は2015年度内、つまり2016年3月までにシステム構築を完了させる」と宣言していました。今回のプロジェクトの骨子の一つは、「標的型攻撃への対策を“速やかに”施す」ことなので、スケジュール通りに構築を終えるのは非常に重要なことです。
今回、最もスケジュール遵守の阻害要因となり得ると予測されたのは、SI業務の量が最も多い「インターネット分離」でした。その際、NECからは、要件を満たしスケジュールも短縮できる方法として「リモートデスクトップサービスを活用したインターネット分離」が提案されました。当時、インターネット分離にリモートデスクトップサービスを利用する方法は新しい取り組みでしたが、NECの過去実績とノウハウをもとに短期間・低コストで実装できました。その結果、システム構築をスケジュール通り終えることができました。NECの提案力は評価に値します。

ソニー損害保険株式会社 様

先行ユーザーからのアドバイス

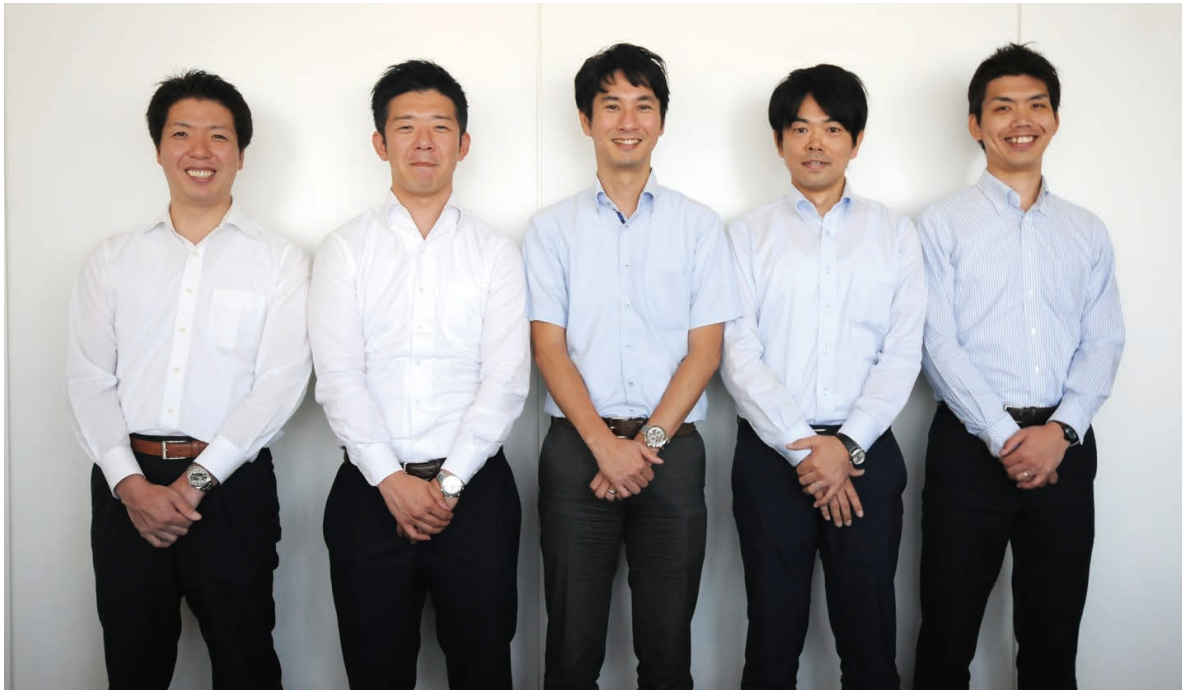
標的型攻撃対策の強化を検討している組織・企業に向けて、「先行ユーザーとしてのアドバイス」があればお聞かせください。

セキュリティ対策は、「制約ありき」の施策だと考えます。それを行って何かの機能やパフォーマンスが向上するということはなく、実施すれば必ず制約が発生します。その制約を最小限にする努力は必要ですが、それでもゼロにはなりません。
セキュリティ対策が本来的にこうした性質の施策である以上、プロジェクトの推進にあたっては、各現業部門へのタイムリーかつ適切な事前説明、そしてプロジェクト途中での柔軟な調整が不可欠になります。今回のプロジェクトでも、やはり現業部門とのコミュニケーションの重要性を再認識しました。
また、「制約を最小限にしていく」という意味では、ユーザーが最も気にする制約は「使い勝手」なので、これをなるべく変更しないよう努力することが重要です。使い勝手を変えないとは、つまり「従来と比べたときの操作・運用の『手順』に変化が生じないよう図る」ということです。

今後の期待

NECへの今後の期待をお聞かせください。

ソニー損保では、今後ともお客様情報を厳格に管理・保全するべく、セキュリティ対策の強化へ継続的に取り組む所存です。NECには、そうした弊社の取り組みを、優れた技術、製品、提案を通じて、後方支援いただくことを希望いたします。今後ともよろしくお願いします。



写真左から：
NEC　第三金融ソリューション事業部　マネージャ　野島 亮一 ／ ソニー損害保険株式会社　システム企画部　技術企画課　主査　渡部 陽氏
ソニー損害保険株式会社　システム企画部　企画管理課長　松尾 大史氏 ／ NEC　金融システム開発本部　マネージャ　吉田 文也
NEC　第三金融ソリューション事業部　担当　楠本 芳治

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10月現在
Cat.No. B01-16100349J