NTT西日本

NTT西日本が考える 最適な情報セキュリティ対策へのアプローチ

NTT西日本　法人営業本部
ソリューションビジネス部
セキュリティサービス推進室
担当課長　**植田 広樹氏**

NTT西日本　法人営業本部
ソリューションビジネス部
セキュリティサービス推進室
担当課長　**水田 幸司氏**

最適なセキュリティ対策には、「現状把握」と「対策実施計画」が不可欠

2008年2月に警察庁が発表した「不正アクセス行為対策等の実態調査　調査報告書」によると、企業・公共団体は「情報セキュリティ対策実施上の問題点」として、「どこまで行えば良いのか基準が示されていない」(39.3%)、「費用対効果が見えない」(37.0%)、「対策を構築するノウハウが不足している」(36.7%)と回答しており、対策実施上の問題点が浮彫にされた。

『自社の現状が把握できていない状況で、セキュリティ対策を実施しているところに問題があります。最適な情報セキュリティ対策を実施するためのアプローチとして、適確な“現状把握”と最適な“対策実施計画”が不可欠です。』(セキュリティサービス推進室　植田広樹担当課長)

最適な情報セキュリティ対策へのアプローチのイメージ

そのため、NTT西日本は、次のステップで取り組むことが必要と考えている。

ステップ1：把握する項目は漏れなく、ぬかりなく

まずは把握すべき項目を網羅的に洗い出す。セキュリティ対策は全体のバランスが重要で、一つのカテゴリに集中的に実施しても最大限の効果は期待できないためである。

ステップ2：現状を調査し、見えるかたちに

洗い出した項目の現状を把握する。重要な項目については定量化、文書化し、現状を見えるかたちにすることがポイントとなる。

ステップ3：理想とのギャップを知り、問題点を見つける

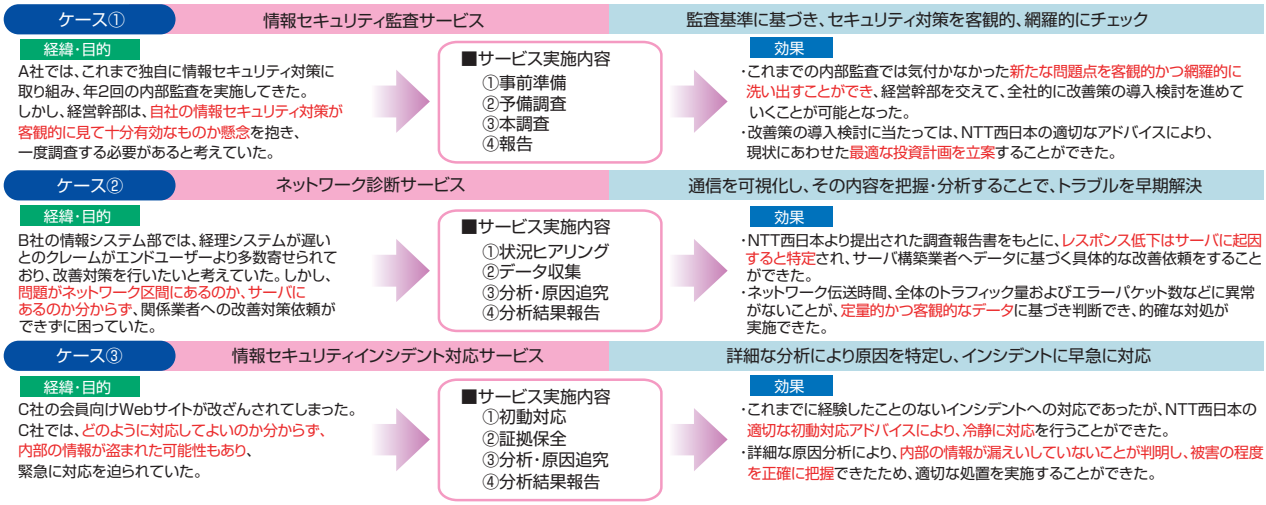
現状を把握したら、自社に何が不足しているのか認識する必要がある。可能な限り客観的に判断することが必要である。

ステップ4：優先順位をつけ、計画的に対策を実施する

確認した問題点に対して優先順位をつけ、何からどのように対策を実施していくか、最適な「対策実施計画」を立てる。リスクの大きさ、発生頻度を考慮し、費用対効果を検討することが最も重要なポイントである。

4つのステップに分けて現状把握と対策実施計画を検討することは、実際にセキュリティ対策を実施するまでに時間やコストがかかり、一見遠回りのように思える。しかし、これらのステップを踏まずに実施する対策は場当たり的なものになり、結果的に過剰な設備投資や、重大なセキュリティインシデントを招く可能性がある。適確な現状把握と最適な対策実施計画が、セキュリティ対策をより効果的に実施するために不可欠であるといえる。

『とはいえ、「考え方は分かるが具体的な方法が分からない」「専任者を置けない」など“自社での実施は難しい”のが現状ではないでしょうか。NTT西日本は、様々なセキュリティサービスの提供実績をもと



想定されるケースとその効果

に、お客様の現状把握と対策実施計画の立案をサポートします。』（セキュリティサービス推進室　水田幸司担当課長）

高度な技術と豊富な実績・ノウハウをもとに、3つのサービスでサポート

最適な情報セキュリティ対策へのアプローチとして、NTT西日本は専門的な分析技術・ノウハウを活用したサービスを提供している。

●情報セキュリティ監査サービス

「現状の対策に漏れがないのか不安」「何から優先的に対策すればよいのか分からない」という悩みを持つお客様には、情報セキュリティ監査サービスが最適である。自組織のセキュリティレベルを高め、顧客の信頼を獲得するためには、網羅的なセキュリティ対策を実施し、維持していくことが必要となる。本サービスでは、豊富な監査経験を持つ有資格者が、自組織では見落としがちな欠陥などを検証し、セキュリティ対策の網羅性・有効性・妥当性を第三者的視点で評価するとともに、改善に役立つ適切な助言を実施する。

●ネットワーク診断サービス

「業務システムのレスポンスが遅いが、問題がどこにあるのか分からない」「ネットワークがつながらないことがあるが、原因が分からない」という悩みを解消してくれるのがネットワーク診断サービス。ネットワークが遅い、つながらないなどのトラブル発生時には、ネットワーク上にどのようなデータが流れているか、正確に把握し原因を分析することが必要となる。本サービスでは、経験豊富なネットワークの専門家が、ネットワークの状況を調査し、不具合の原因などを正確に突き止め、強固なセキュリティ、快適なネットワークを将来にわたって維持するためのサポートを実施する。

●情報セキュリティインシデント対応サービス

セキュリティインシデントに遭遇し、「ホームページが改ざんされてしまい、どのように対応してよいのか分からない」「ウイルスに感染し被害がどこまで及んでいるのか分からない」というお客様には、情報セキュリティインシデント対応サービスが有効である。ホームページ改ざん、個人情報漏えいなどのインシデントが発生した場合は、証拠データの保全を行うとともに、原因の究明と適切な対策を実施することが必要となる。本サービスでは、NTT西日本の専門分析チームが、被害を受けたサーバに対し、証拠データの保全を行い、原因を分析するとともに、再発防止策の提案まで実施する。

各サービスの詳細については、以下に問い合わせをお願いしたい。

お問い合わせ先

西日本電信電話㈱　法人営業本部
ソリューションビジネス部
セキュリティサービス推進室
TEL：06-4803-3690
E-mail：sec-info@bch.west.ntt.co.jp
URL：http://www.ntt-west.co.jp/solution/security/