自動脆弱性診断サービス SCT SECIRE 活用事例

株式会社スカイアーチネットワークス

フルマネージド・ホスティング事業者のセキュリティに対する取り組み

ポイント
- 人とシステムで、漏れの無いWチェック
- 各レイヤーにおける、人材（質・量）の確保
- 診断の対応だけでなく、事前の対策

Company Profile

設立　：2001年7月
社員数：56名
所在地：東京都港区南麻布

株式会社スカイアーチネットワークス 営業本部マネージャーの松田昭穂様にお話を伺いました。

スカイアーチネットワークスは現在、クラウド運用代行、データセンター運用代行、レンタルサーバー運用代行などのサービスを展開しています。分かりやすく言い直しますと、お客様に代わり、サーバーを 24 時間 365 日管理し、お客様サービスの機会損失とダウンタイムの最小化を行う**サーバーの管理屋さん**をやっています。

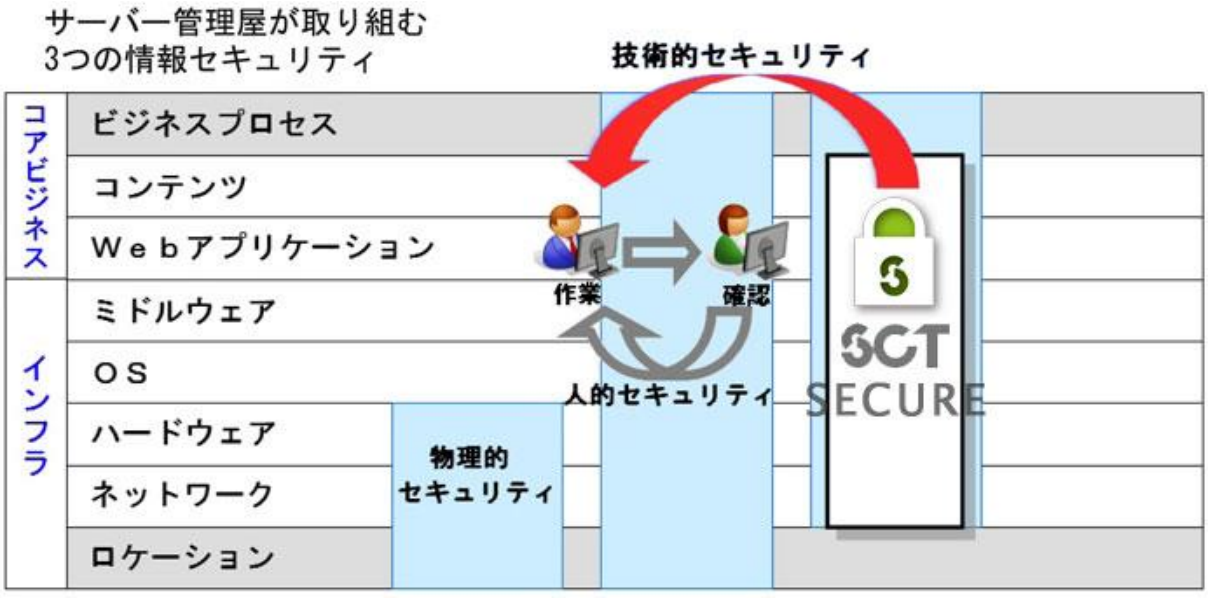
～８つのレイヤー～

サーバーの管理屋ということでサーバーの管理・構築の業務を行うわけですが、セキュリティにつきましては、８つのレイヤーを想定し、そのレイヤー毎に対策を行っております。ここでいうレイヤーとは、サーバーの「ロケーション」、「ネットワーク」、「ハードウェア」、「OS」、「ミドルウェア」からなる「**インフラ部分**」、そのサーバー上に乗る「Web アプリケーション」、「コンテンツ」、「ビジネスプロセス」からなる「**コアビジネス部分**」です。スカイアーチはこの内のインフラ部分をサポートしています。

～人材確保～

レイヤーそれぞれのセキュリティについてですが、最下層のロケーション以外については、**人的セキュリティ**をもって対応します。人的セキュリティとは、それぞれのレイヤーの専門家によるセキュリティ対応のことを指します。また、ネットワーク、ハードウェア、OS、ミドルウェア、Web アプリケーション、コンテンツの６つのレイヤーに対してはさらに加えて SCT SECURE による診断を行っています。人的セキュリティ対策の漏れをなくし、管理レベルを上げています。

セキュリティ対策については、各レイヤーの専門家たちが作業の中で確認します。**専門家によるチェック**はセキュリティを確保する上で大変重要ですし、お客様に安心感をもって利用していただくための欠かせない要素です。しかし、人によるチェックの場合、どうしても見落としや抜けの可能性が出てきます。また、最新のセキュリティ情報の収集などに時間がかかってしまい、実際のセキュリティ状況とのタイムラグによるギャップが生じる場合があります。



弊社では、このような**人的セキュリティを補完するものとして、技術的セキュリティ＝脆弱性診断ツールを活用**する事を重要視しています。

～Wチェック～

各レイヤーの専門家が作業をし、それを別の人間がチェックします。それに加え、第三者機関である SCT SECURE によるチェックが行われます。サイトを運営されるお客様がウェブサイトの安全性を判断する材料として、このような第三者のチェックが有効です。各レイヤーの専門家の視点も大切ですが、**お医者さんのセカンドオピニオンのように違う視点で診断してもらう**ことが大切だと考えています。

違う視点からのチェックを複合的に行うことで、脆弱性を防ぐことが可能になります。人のチェックを補うものとして自動診断によるチェック、自動診断のチェックを補うものとして人によるチェックと、判断があります。

例として、弊社インフラエンジニアの行うセキュリティ対応の一部を見てください。

1．ＯＳなどのバージョン最新化
2．パッチ（修正プログラム）適用
3．不要サービスや機能の停止
4．不要なアカウント削除、パスワード強化
5．ディレクトリなどのアクセス権設定
6．ログ設定

この対応に対し、別のエンジニアがチェックを行います。セキュリティ状況は日々変わっているので、インフラエンジニア側もまた日々チェックを行っています。しかし、例えばいったんパッチ適用に関する情報が漏れてしまうと、脆弱性をつかれた攻撃が起こり得ます。そして、人間が行うことには漏れがあります。ここで脆弱性診断ツール SCT SECURE を利用することで漏れを無くし、安定した運用に繋げています。

～事前対策～

発見された脆弱性に対応することはもちろん大切ですが、**もっと大切なのは、未然に防ぐ対策を行うこと**、これがサービス提供を行う上でキーポイントとなります。脆弱性はいつ発生するか分かりません。いったん発生したときに、対応を急ぐあまり、充分な調査をせず場当たり的な対応をしてしまうと、常に場当たり的な対応にならざるを得なくなります。これに対し、弊社では**プロアクティブ（先手）な対策**をとっています。例えば、日々の運用で対策しておくべきバージョンアップなどのセキュリティ情報を取り入れて、問題がない状態を維持しています。その上で脆弱性が発見された場合の対応ノウハウを手順化し、スケジューリングして時間を確保した上で、改修と確認を慎重に行っています。

～SCT SECURE サービス提供・無料診断～

冒頭で弊社のサポート範囲はインフラ部分と言いましたが、サービスとして、アプリケーションとコンテンツのコアビジネス部分に対しても IPS や WAF による防御、さらに SCT SECURE による脆弱性診断を提供しております。また、SCT SECURE を利用した Web サーバーの脆弱性の有無、危険度をお知らせする**無料 Web 診断**（http://web-shindan.jp/）も提供しております。