ITmedia エンタープライズ セキュリティセミナー:

「自分たちでできないことはやらない」　分業でセキュリティ強化を図る「京王SIRT」

http://www.itmedia.co.jp/enterprise/articles/1802/27/news009.html

54社のグループ企業の中核を担う京王電鉄。横断的セキュリティを実現するために立ち上げたCSIRTで、どのような取り組みをしているのか。

2018年03月13日 12時00分 更新

[タンクフル, ITmedia]

　54社のグループ企業の中核を担う京王電鉄。横断的セキュリティを実現するために立ち上げたCSIRTで、どのような取り組みをしているのか――。ITmedia エンタープライズが2017年11月に開催したセキュリティセミナーで、同社の経営統括本部 IT管理部長を務める虻川勝彦氏が「京王SIRT」の取り組みについて講演を行った。

「ゼロ地点」から始まった横断的取り組み――京王電鉄

京王電鉄 経営統括本部 IT管理部長　虻川勝彦氏

　2009年から2010年にかけて猛威を振るったマルウェア「Gumblar（ガンブラー）」を覚えている人は多いだろう。京王電鉄も当時、外部業者に委託して制作、運用していたキャンペーンサイトが改ざんされたという。

　虻川氏は、当時を「外部公開Webページの一括管理をしていない状態で、グループ各社や各部署が個別に作成、管理していた」と振り返った。要するに、各社が個別に構築した公開サイトを把握しきれていない状況下でのGumblar感染。これが契機となって、「ゼロから」の「横断的なセキュリティ対策」に着手したという。

　同社では、外部公開Webページを全て把握するため、グループホームページ分科会を設置し、外部の制作側も巻き込んで管理状況をチェックするための体制を整えた。また、全Webページに改ざんチェックツールを導入。外部委託先に対してはチェックリストを作成して問題点を洗い出し、改善の依頼や委託先の切り替えを実践した。

　54社のグループ企業の中核を担う同社では、グループ企業の統制も求められる。虻川氏は、「“ガバナンスは押し付け”と感じて反発する人もいる。そこで、ガバナンスという表現ではなく、メリットや“お得感”を出して、共感して利用してもらうというアプローチをとった」と、独自の取り

組みを紹介した。

さまざまなセキュリティ施策を実施するに当たり、「グループ各社の負担を軽減するため、ベンダーとの価格交渉やボリュームディスカウントの導入はもちろん、“工数削減のために自分たちが汗をかく”など、コスト削減に奔走。必要なものを安価に調達し、きちんと使ってもらうことに取り組んだ」と説明した。

京王SIRT・京王セキュリティポータルで横断的セキュリティを強化

同社では、横断的セキュリティに対する取り組みをより強固にするため、2015年7月16日に「京王SIRT」を設立。2017年4月にはグループ会社の連携ツールとして「京王セキュリティポータル」を稼働した他、クラウドの積極的導入を進めながら、Webページの構築ガイドの作成に着手した。

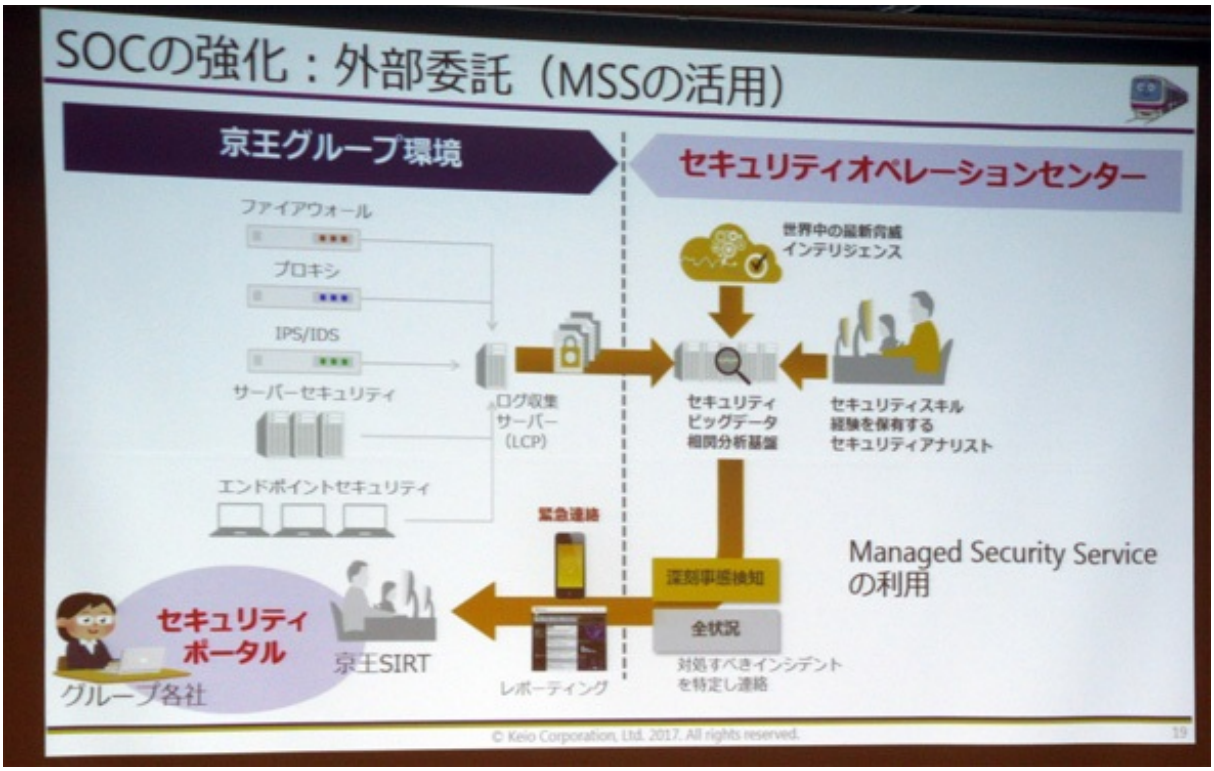
京王SIRTでは、SOC（Security Operation Center）の体制強化が課題だったという。「どうやってインシデントの検出精度を高めるか、セキュリティ監視の運用負荷を軽減するか、体制を維持し続けるかという課題に対し、やるべき事に注力するために、『自分たちで必要なレベルまでできないことはやらない』と決めて、外部事業者が提供するMSS（マネージドセキュリティサービス）を活用。ファイアウォールやプロキシ、IPS/IDS、エンドポイントのログを監視、分析してもらっている」（虻川氏）。インシデントが起こった場合の対応については、セキュリティポータルを介してグループ各社で情報共有しつつ進めるという運用になっている。

クラウドについては、当時、同氏が在席していた京王バスが2011年から順次導入を進めている。虻川氏は、「システムが停止しても業務への影響が低いシステムから開始した『検証期』から、多くの人が触れてクラウドは使えるという認識を広める『導入期』を経て、基幹システムに導入する『活用期』へ進んだ」と流れを説明。2016年3月には全国のバス会社や一般ユーザーに使ってもらっている高速バス予約システム「ハイウェイバスドットコム」を「AWS」（Amazon Web Services）に切り替えたという。

京王電鉄でも、2015年末からクラウド活用を始めている。セキュリティの強化やBCP対策の観点からもクラウドを推進。「迅速かつローコストなDR（ディザスターリカバリ）環境の構築に向けて、クラウド活用へ舵を切っている」と述べた。

最後に虻川氏は、経営層や上司に「セキュリティの必要性」を説明する際のポイントを紹介した。

「経営層の中には、『セキュリティは金食い虫』『セキュリティ対策は金を生まないので積極的にやりたくない』と考えている人も少なからずいると思う。こうした相手には、理解度や意識、会社の状況に合わせて分かりやすく表現を変えるのが大事。経営層はさまざまな部門の話を聞くため忙しく、興味のないことは記憶に残りにくい。以前に説明したことでも覚えていないことを前提に、聞き手の立場に立って説明すれば通じることも多い」と強調した。そして最後に来場者に向けて、「あまり考え過ぎて動けなくなるより、できるところから始めよう」とアドバイスを送り、講演を締めくくった。



横断的なセキュリティ実現のために外部委託も有効な選択肢だ

クラウドで安全・確実にIDを管理　病院向けソリューションにも応用

日本オラクル クラウド・テクノロジー事業統括 Cloud Platformビジネス推進本部シニアマネージャー　大澤清吾氏

　ランチセッションでは、日本オラクルの大澤清吾氏とリコーの谷口竜氏が、両社のサービス連携について説明した。

　日本オラクルの大澤氏は、現在、同社が注力しているクラウド環境でのセキュリティについて説明。要となるのは、IDとパスワードの管理だ。大澤氏は、同社が2017年1月に発表したクラウド型のID管理サービス「Oracle Identity Cloud Service（Oracle IDCS）」の優位性を説明した。

　Oracle IDCSの特徴は、オラクルが提供するSaaS／PaaS／IaaSはもちろん、GoogleやMicrosoft、Salesforce、Boxなど、ビジネスシーンで活用されている主なクラウドサービスに対応していること。クラウド上でIDを管理することで、シングルサインオンでそれぞれのサービスをストレスなく利用できるようになる。

　企業がクラウドを利用する上で頭を悩ませている、ユーザー認証／認可、ユーザー管理などの機能を利用できるため、セキュリティを含めた対策が可能になるという。

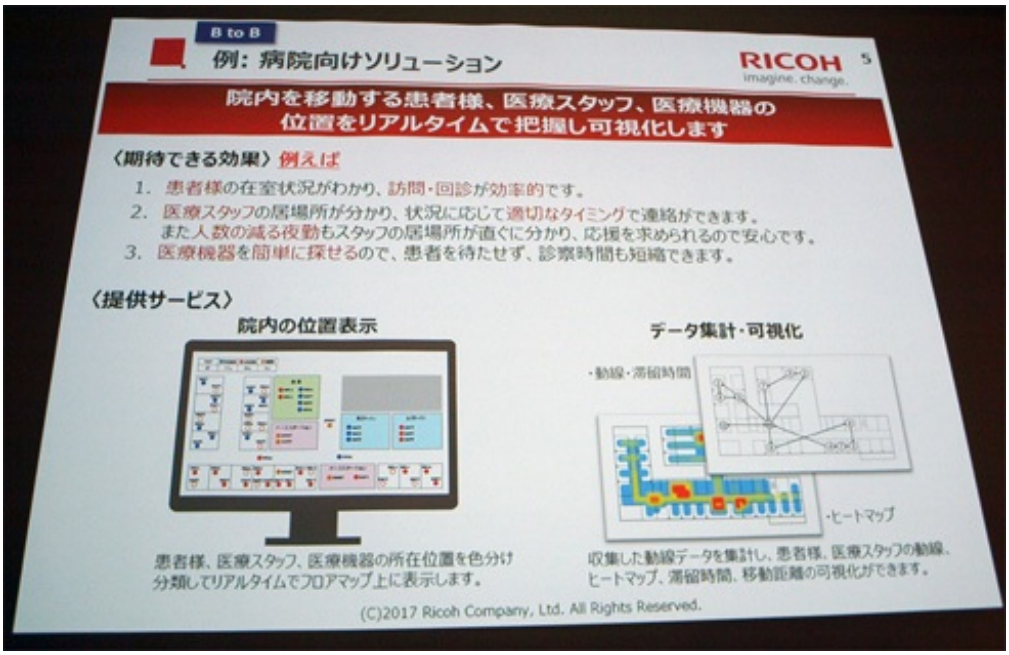
病院向けソリューションのIDを「Oracle IDCS」で安全に管理

リコーの谷口氏は、同社が提供しているセンシングソリューションの事例を紹介した。事務機やカメラのメーカーとして知られ、さまざまなITソリューションの提供でも実績があるリコーは、講演で病院向けのソリューションと街づくりに関するソリューションについて説明した。

リコー オフィスサービス事業本部 ワークプレイスソリューションセンター サービスプラットフォーム開発室　谷口竜氏

病院向けソリューションは、院内の患者やスタッフの位置を可視化するもの。電子カルテとの連携も可能で、医療業務の効率化や改善に役立つという。これらのソリューションはセキュリティと密接な関連があり、そこで利用しているのが、Oracle Identity Cloud Serivece（IDCS）だ。

リコーでは、パブリッククラウドをベースにしたソリューションの提供にシフトしているという。ID管理をクラウド上のIDCSで行うことで、認証や許可を一元管理できる。さらに既存のアカウントを利用して他のサービスを利用できるため、ユーザーの利便性も向上すると説明した。



リコーの病院向けソリューションの例。患者の在室状況やスタッフの居場所をリアルタイムで可視化。医療サービスの効率化に役立つという

「暗号化された添付ファイル」による標的型攻撃を無効化するには？

クオリティア 営業本部 ソリューション営業部 部長　辻村安徳氏

昨今、メールに関する脅威が多く伝えられている。クオリティアの「Active! zone」は、そのメールを安全に扱うためのソリューションだ。同社営業本部 ソリューション営業部で部長を務める辻村安徳氏はまず、年を追うごとに標的型メールの仕組みが高度化し、脅威が増している現状を説明した。

標的型メール攻撃は、ネットワーク上やエンドポイントで防御しようという考え方が一般的だが、辻村氏はネットワーク上に統合型のファイアウォールやUTMを設置し、個々のエンドポイントに対策を施すのは「多大なコストと手間が必要になる」と指摘する。

場合によってはエンドポイント保護のアプリをインストールするためにPCのスペックを上げる必要に迫られることもあり、社内の全てのPCで対策が完了するのに時間がかかるなどの問題点を指摘した。

そのうえで、最近の傾向として辻村氏が挙げたのが、「暗号化された添付ファイル」による攻撃だ。

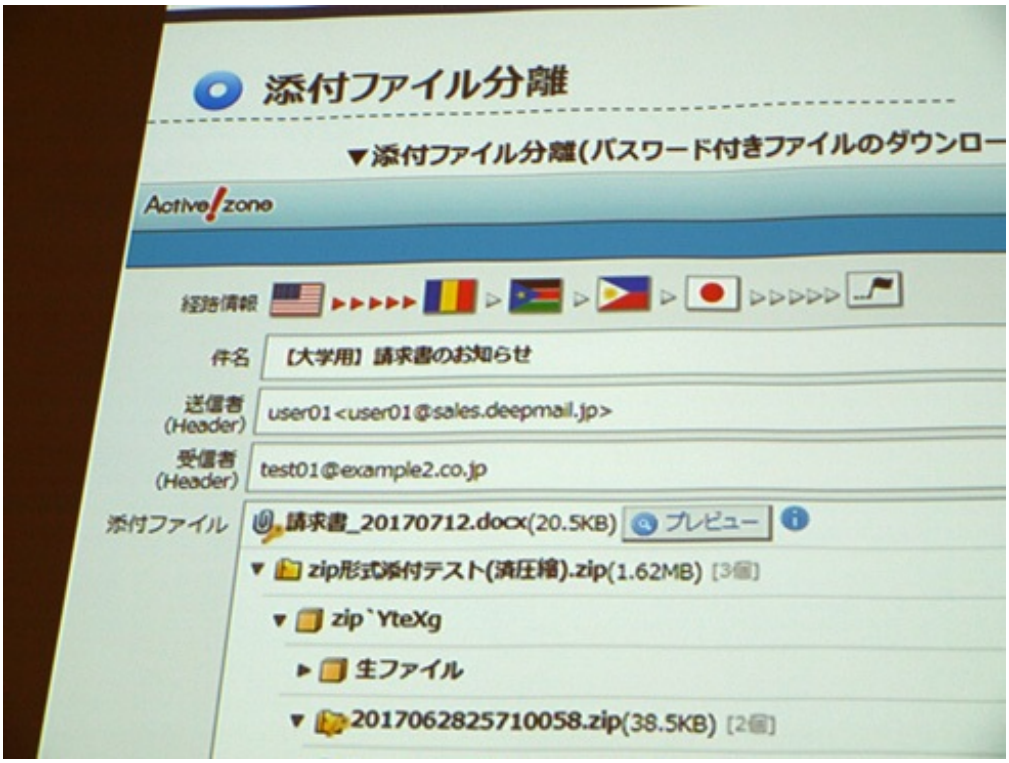
最近のビジネス現場では、ZIPファイルなどを暗号化してメールに添付するシーンが増えている。その暗号化されたファイルが、“暗号化されていることで”ネットワーク上のセキュリティをすり抜けてしまい、エンドポイントに到達してまうことがある。そこで、パスワードを使って開封されると、マクロが動き出す。

Active! zoneは、このような場合に添付ファイルによる攻撃を無効化できると辻村氏は説明する。Active! zoneは、メールに添付されたファイルに対し、マクロ除去や画像化などを行うことで、悪意のあるマクロの実行を回避する。

例えば、マクロが仕込まれたPDFファイルも、画像化すればマクロは動かない。しかも、画像なので閲覧が可能だ。ほかにもActive! zoneは、HTMLメールのテキスト化や添付ファイルを分離して画像化し、その内容を確認してからでないとダウンロードできないようにする機能も備える。講演ではその操作デモも行われた。

辻村氏は、同ソフトは自治体で多く利用されていると説明。価格面での優位性を訴えて講演を終えた。

エンドポイントにサンドボックスを入れるには、ある程度のスペックのPCが必要。暗号化された添付ファイルによる攻撃は増えている



「Active! zone」の画面。画面左上にメールの経路が国旗で示される機能も備える。3つ以上の国を経由するメールは危ないという

関連記事

新たな技術の出現でサイバー犯罪はどう進化する？　インターポールが示す未来の攻撃

あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度化するとともに、ますます深刻化が予想されるサイバー脅威に対し、企業はどのような対応策を講じるべきか？――国際刑事警察機構（インターポール）という国際機関の視点から見たセキュリティ事情に、そのヒントを探る。

FBIも警鐘! ファームウェアを狙った攻撃が急増
ますます深刻化するサイバー攻撃の脅威に対し、企業はどのような体制で臨めばいいのか。「ITmediaエンタープライズ セキュリティセミナー」から、そのヒントを紹介する。

“役員も巻き込んで”危機意識を共有　ジャパンネット銀行の“脅威を自分ごと化させる”CSIRT
サイバーセキュリティに関するさまざまな取り組みで知られるジャパンネット銀行。2013年に立ち上げた「JNB-CSIRT」は、役員も訓練に巻き込んで危機意識を共有するなど、サイバー攻撃を“自分ごと化”する活動が特長だ。

アクサ生命のCSIRT、“本気の”サイバー演習で見えた課題
ITmedia エンタープライズ主催のセキュリティセミナーで、アクサ生命のCISOが登場し、CSIRTとサイバーインシデントレスポンスの取り組みを紹介した。同社では情報漏えいなどのシナリオを想定した“本気の”演習を毎年行っているという。

世界200拠点を守るヤマハ発動機のCSIRT、体当たりで挑んだ「セキュリティガバナンス」
グローバルな視点でサイバー脅威からどう企業を守るかーー。ITmedia エンタープライズが11月に開催したセキュリティセミナーでは、ヤマハ発動機におけるCSIRTの取り組みや、セキュリティ対策のトレンドである「Threat Hunting」が紹介された。

ITmedia Inc.