事例

[株式会社山梨ニューメディアセンター]

グループ各社の端末を一元管理 ユーザーの意識向上も重要

グループ会社の情報セキュリティ対策では、システム面とともに各社の利便性やユーザーの意識向上といった視点も重要になる。各社でサービスに対する考え方が異なるからだ。山日YBSグループのICT業務を担う株式会社山梨ニューメディアセンター（以下、YNMC）は、山日YBSグループの情報系ICTインフラの刷新に伴い、各社の端末を一元管理しセキュリティの強化を実現。端末にデータを残さないなどシステム面での改善とともにユーザーの意識向上も図っている。

右側から順に
代表取締役社長 **西川 勝仁** 氏
企画開発局 ソリューション事業部 副部長 **髙岸 道男** 氏
企画開発局次長 **望月 裕** 氏

山梨日日新聞社と山梨放送を中核とする山日YBSグループは、総合メディア情報グループとして140年にわたり山梨県民とともに歩み続けている。電子版の朝・夕刊を発行するなどデジタル化が進む同グループで、ICT業務を担っているのがYNMCだ。同社はグループ内の基幹業務システムなどの開発・運用にとどまらず、県内の行政業務システムや旅行業支援システム、デジタルサイネージといったパッケージの提供などICTを駆使し山梨県の発展に貢献している。

メディアの世界で事業を展開する同社にとって、情報セキュリティ対策は重要な経営課題である。ネットワークに関しては、インターネットに接続する情報系と社内に閉じている業務系の2つに分けている。さらに新聞記事に関わるシステムを独自のネットワークに分離することで、改ざんや個人情報保護の対策強化を図っている。

西川氏によると、2012年6月、安定性の向上とセキュリティの強化を目的に刷新した情報系のICTインフラにおいて、セキュリティ面でのポイントは大きく3点あった。1つめは、グループ各社の本社と支社間をVPN接続で結ぶ情報系ネットワークの統合。営業部門などの外部からのアクセスに対して、内部ネットワークと同等のセキュリティを保持できるようになった。

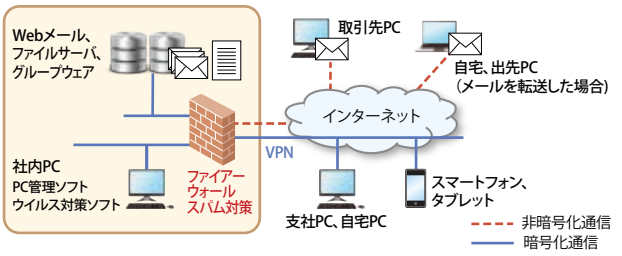
2つめは、PC管理ソフトを活用した情報系端末の一元管理だ。この結果、各社の端末のリアルタイムな状況や未使用端末の把握が可能となり管理外の端末は接続できない。またUSBメモリにファイルをコピーした場合もPC管理ソフトによりログが残るため、情報流出の抑止力となり万一のときも影響の最小化が図れる。

3つめは、端末にデータを残さないことを目的とするファイルサーバとWebメールの導入だ。サーバ側でメールのデータを一元管理するWebメールを利用することで、端末がウイルスに感染した場合もメールやアドレス帳などの悪用を防止できる。

グループにおけるセキュリティ対策の課題について髙岸氏は「グループ各社でセキュリティの考え方は異なっている。グループのセキュリティポリシーの策定では各社の中でセキュリティレベルの高い方に合わせることを基本にしているが、具体的に対策を実施していく段階では各社の利便性への配慮も重要」と話す。モバイル端末の活用は各社の判断に委ねているが、利用端末はすべてYNMCが中身をチェックしグループセキュリティに準じた設定を行う。また、YNMCがVPNソフトをインストールし、いつどこにアクセスしているのかを把握可能にしている。

「どんな仕組みでも100%の安全を得ることはできない。大切なことはセキュリティ対策の重要性をユーザーに理解してもらうこと。通常、ユーザーへの啓発活動はトップダウンによる情報伝達とメールでの周知が基本だが、今後は防災訓練と同様にサイバー攻撃訓練を行うなど、万一感染したときに何をすべきかを体感できる教育も必要になると考えている」と望月氏は話す。

サイバー攻撃が巧妙化する中、グループ全体でシステムによる防御とユーザーの意識向上を図っていくこうした取り組みは、今後も継続し強化することが必要だろう。



注：取引先PC、メール転送もファイルの暗号化を推奨

Webメールの利用形態

会社概要
株式会社 山梨ニューメディアセンター
所在地　〒400-8545 山梨県甲府市北口2丁目6-10
URL　http://www.y-nmc.jp/
事業内容
アプリケーションソフトウェアの開発・供給、情報システムの運用・保守、ホームページ制作、インターネット接続サービス、サーバハウジング・ホスティングサービス、パンチによるデータ入力・加工・出力、情報関連機器販売・設置工事、前記の付帯サービス