NECのセキュリティソリューション群のフォレンジック分野を担うNetEvidence

日本電気株式会社
キャリア・プロバイダー事業部
ソリューションビジネス推進部マネージャー　新江俊史氏
キャリア・プロバイダー事業部
ソリューションビジネス推進部主任　海老名和夫氏
エネルギーソリューション事業部
ソリューションビジネス推進部マネージャー　大貫克巳氏

情報セキュリティ管理技術の中でも，近年特に注目されているのがフォレンジックテクノロジーだ。NECは同社のセキュリティソリューション群「iBestSolutions/Security」のフォレンジック分野を担う製品として，オーク情報システムが開発した「NetEvidence」に白羽の矢を立てた。NECのセキュリティ担当者に聞いた(編集部)。

フォレンジック機能を確保した

本誌　NECがNetEvidenceを扱うきっかけは？

新江　私どもの部署は，IT・ネットワーク統合を実現する“UNIVERGE(ユニバージュ)”を中核としたブロードバンドソリューションビジネスを担当するグループに所属しています。言うまでもなく，ブロードバンド技術は，今日のビジネスの基盤となるもので，セキュリティシステムも例外ではないと考えております。

その中でもフォレンジック分野は，ブロードバンドネットワークと密接な関係を持つものだと認識しており，私どもの部署で扱うことが最適だと考えました。

海老名　情報セキュリティの分野は，当初コンピュータウィルスへのリスク対策など，外部から脅威に備えることから始まりましたが，最近では専ら，組織内部の関係者による不正アクセス対策など，内部からの情報漏洩の脅威に備える動きも活発になってきています。

NECとしても，PCの操作ログの採取，メールによる情報漏洩対策を検討してきましたが，より厳しい情報漏洩の対応策として，NetEvidennceの機能に着目した次第です。

新江　NECは，「iBest Solutions/Security」という統合セキュリティソリューション体系を整備し，お客様に提案してきています。その統合体系を構成する一つの要素としてフォレンジック分野が最近注目されていますが，その具体的な対策ツールであるNetEvidenceの重要性を認識し，昨年８月より本格的に販売を始めています。

取り扱い開始から１年余りですが，すでに数千人規模の大企業を中心に，複数の企業への導入実績を持つに至っています。

本誌　NetEvidenceに惹かれた理由は・・・。

海老名　フォレンジック製品を導入する本来の目的は，情報漏洩が起きた場合に，それを引き起こした人物を特定すると同時に，情報の流出ルートを特定することにあります。これを実現するためには，絶対にログ情報の記録漏れがあってはなりません。さらには長期にわたって，ログ情報を保全しておく必要があります。

加えて，蓄積されたログ情報を素早く分析できる機能も必要不可欠とされています。

NetEvidenceは，これらのすべての必須機能を合わせ持つことから，お客様が本当に使える製品だと判断しました。ちなみに，数世代に渡る記録情報を横断的に解析できますし，Eメールなどは添付ファイルも含み全文検索できるなど，フォレンジック製品として十分に満足していただけるシステムだと考えております。

証拠能力のあるログ情報

新江　現時点ではすべてのユーザーが，フォレンジックという分野を正確に理解しているわけではないでしょうが，私どもはフォレンジックの一番のポイントは，生の証拠を完全な形で保全することにあると認識しております。

たとえば，フォレンジック製品として提供されている多くのものは，不正処理が行われた時，何らかの痕跡を部分的に記録する形を採っています。具体的には，何時，誰が，どういった操作を行ったかというような操作や処理の内容や経緯をテキストなどに変換して記録しておくものがほとんどです。

これらテキストなどに変換された情報が，はたして実際の証跡ログとして最適なのかという疑問を常に抱いてきましたが，やはり証拠として最適な形は，ネットワーク上を流れた生の情報をパケットの形で記録しておくことが，本来の姿であるし，本当の意味での証拠能力のあるログ情報ではないかと考えています。

海老名　ちなみに従来のログ記録ツールは，不正を抑止するためのもの，NetEvidenceは不正が行われたことを証明する証拠情報を記録しているということだと思います。

本誌　証拠を保全するというフォレンジックの本来の目的を理解しているユーザーには，NetEvidenceの機能が高く評価されますが，フォレンジックに対して深く理解されてない場合は，そこまで必要なのかということになりませんか。

大貫　この両者の違いが生まれる背景は，やはりユーザー企業内にセキュリティに対する認識が十分あり，社内体制が整備されているかという点にあると思います。


大貫克己氏


海老名和夫氏


新江俊史氏

さらに上位のフォレンジックへ

本誌　さて，NetEvidenceに対する要望は・・・。

海老名　フォレンジック製品としての必要な機能を持っていますので，基本的機能については満足しております。導入したユーザーから高い評価を得ていますし，私どもも自信を持っています。

しかし，ネットワーク全体の運用管理という視点まで拡げていくと，今後必要になってくる機能もあると考えております。たとえば，NetEvidenceを運用しているサーバーの死活監視機能，つまりフェイルセーフ機能の拡充などです。

現在NetEvidenceのサーバーが正常に稼働しているか否かを確認する方法は，NetEvidence側から定期的に送られてくるメールによって判断しています。NetEvidenceのサーバーが何らかの理由でダウンすると，定期的なメールが送信されなくなり，そこで初めてサーバーのダウンが判明します。

ところが，大規模なネットワークを運用している企業にとっては，受動的なサーバー管理では満足できず，全体を運用管理する側からサーバーを能動的に管理したいという要望があります。

そこで，NetEvidenceのサーバー側に管理システムに対応したインターフェイスを設けてもらいたいと感じています。

新江　もう一つ，これはオーク情報システムさんだけでなく，私どもNEC側も共同して対応すべき点だと思いますが，個人認証の製品との連携を強化していかなくてはならないと思っています。

NetEvidenceに記録された情報と，その情報を操作／作成した個人を正確に特定することが，その情報の証拠能力としての精度を高めることになると考えるからです。

大貫　これらの要望は，私どもが営業と共に自らユーザーのところへ行き，生の声として伺っているからこそ分かったものです。セキュリティ対策を実施している現場での生の声を真摯にうけとめ，オーク情報システムさんへの要望だけでなく，私どもNEC側で対応することも含め，フォレンジックシステムのよりよい発展につなげていきたいと考えております。

日本電気株式会社
〒108-8425 本社 東京都港区芝5-33-1
森永プラザビル
tel.03-3798-6012
http://www.nec.co.jp/