ユーザーニーズを反映 さらに上位レベルを狙えるNetEvidence

株式会社インターメディアシステム　システム部課長　**米廣正雄**氏
株式会社オーク情報システム　セキュリティ事業部長　**梅田高久**氏

機密情報漏洩者をつきとめる！

企業内ネットワーク上を流れるあらゆるデータのログを取得する「NetEvidence」。この製品を活用して社内情報システムのセキュリティを向上させているのは，「温泉」をキーワードにシニア世代に対してコンテンツを提供し，急成長を遂げている広告・旅行業の（株）インターメディアシステムである。同社の情報システムセキュリティ担当者の米廣正雄氏と「NetEvidence」を提供する（株）オーク情報システムのセキュリティ事業の責任者である梅田高久氏に聞いた。


米廣正雄氏

Pマーク取得のためのNetEvidence

本誌　インターメディアシステムの会社概要から教えてください。

米廣　具体的には，温泉・宿・街情報を紙媒体「名湯ゆこゆこ」やインターネットサイト「ゆこゆこネット」で発信し，シニア世代に「遊び」を提案している企業です。

本誌　NetEvidenceを導入したきっかけは？

米廣　大前提として，最初にNetEvidenceという製品ありきではありません。

業務内容から，プライバシーマークの取得が不可欠ということで，そのためには社内の情報セキュリティ対策を推進する必要に迫られました。

そこで，まずは社内の情報がどのように流れているのかを掴むことが大きな前提となり，（そのためには）情報のログをとることを最優先だと考え，NetEvidenceを導入した次第です。

本誌　当初からNetEvidence一筋で？

米廣　いいえ，そんなことはありませんよ。競合他社の製品を含めて，様々検討した上で，最終的にNetEvidenceの導入を決めました。

やはり決め手となった機能は，スケジューリングの機能が充実していたということですね。これは，他社の製品にはありませんでした。

私どもの業務では，「名湯ゆこゆこ」という隔月刊の雑誌を発行している関係で，その発行のピーク時に社内ネットワークの情報量が，通常と比較して膨大になることがあります。

そこでNetEvidenceでは，2台の管理サーバーが予め決められたスケジューリングに沿って自動的に切り替わりながら，24時間体制で継続的に運用できる点に注目しました。

ログ情報をデータベース化

梅田　NetEvidenceには，様々な特徴ある機能を備えているのですが，今おっしゃっていただいた機能は，私どもが自信を持っておすすめしているものとなっています。

と言いますのも，ログ採取を基本機能にするシステムでありながら，実際には，記録容量をオーバーフローしていまい，ログを採取しているつもりが，実は取れていなかったという事例の報告も結構あるのが実状なのです。

その意味で，確実にログを取得できるための要の機能として，ご指摘の部分は多くのユーザーの皆様に，ご評価いただいている点になっています。

本誌　製品機能への満足度はいかがですか？

米廣　もちろん基本的な機能については満足しています。ネット上を流れるすべての情報のログを取得し，データベース化してくれますし，合わせて提供されている検索機能を利用して，情報漏洩につながるような行為の有無を含めて，様々に分析できる機能はたいへん重宝しています。

梅田　ご評価，ありがとうございます（笑）。

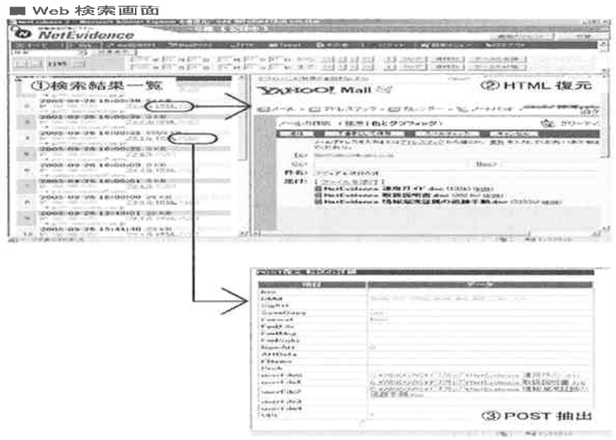
米廣　とは言え，すべての機能で完全に満足しているかというと，平均点以上ではあっても文句の付け所がないということがありません（笑）。

基本的な機能が素晴らしいだけに，使い勝手という面で，もう一歩進めてくれたら，さらに高く評価されるだろうという点がいくつかありますね。

たとえば，2台の管理サーバーをスケジューリングし，自動的に切り替えられる機能がありますが，


梅田高久氏

検索項目設定画面



Web検索画面

現時点では，予め任意に決められた日時によって切替えが行われる機能になっています。

毎月の業務がほぼ一定の場合ならば良いのでしょうが，私どものように，ある月は比較的情報量が少なかったと思うと，行楽シーズンや隔月の情報誌の発行がある期間には，情報量が格段に増えるということもあります。

それを日時だけで切替えが行われてしまうと，一方の記録データは少ないが，一方の方には膨大なデータが記録されているということが起きてしまいます。

この点について，可能であれば記録される情報量がある一定の量を超えたときに切り替わるといった利便性を持たせてもらえましたら，より高い評価をつけられると思います。

梅田　まさにそのご指摘は，将来的に是非とも私どもでも製品の中に組み込んでいきたいと思っております。

100倍速の検索エンジン登場

本誌　評価しているのは，どのような点ですか？

米廣　NetEvidenceの最大の特徴の１つが，ただ単にログを取得するだけでなく，ログ情報を検索できる形で自動的にデータベース化してくれる機能を持つことです。これによって，誰もが自由に様々な形で分析できるわけですが，この機能については，実に素晴らしいと思います。

梅田　ログ情報を取得し，蓄積していくだけの同種のツール／システムがありますが，ご指摘していただいた点は，他社のものと一線を画しているものと，私どもも自負しているポイントです。

米廣　ただ，データベース化された情報を分析する時の検索スピードが弱冠遅いところが気にかかっていました。

梅田　これも先駆ユーザーからご指摘を受けたご要望でしたが，先頃発表しましたNetEvidenceのバージョン２（Ｖ２）で，解消しておりますので，是非ともお使いいただきたく思います。

これまでも，検索データのヒット数が少なければ問題なかったのですが，対象が多くなるとかなり時間がかかってしまい，ご不自由をかけていたと思います。

ちなみにＶ２では，検索ロジックを見直し，意味の少ない割り込み作業や無駄なルーチンを排除するなどで，かなりの高速化を実現しています。

こうした改良と合わせて，新たにオプションとして「高速検索エンジン」を開発，提供を開始しております。

本誌　どれくらいの高速化が実現されますか。

梅田　インデックス検索では，従来の100倍以上の高速処理が期待できる優れものとなっています。

米廣　NetEvidenceには，予め設定した語句を検知すると，直ちに情報漏洩の可能性があるデータとして検出し，それを管理者に警告メールという形で送付してくれる機能があります。この機能はとても重要だと感じておりますし，基本機能としては大変満足しています。

ただ，語句の設定によってはとんでもない量の警告メールが来てしまうことがあり，それを一つひとつチェックしていくだけでも，大変な作業になってしまうことがあります。

また，警告メールを分析していくと，そのほとんどが社内メールであり，通常業務の情報活用の中で利用されているだけということが多いのです。

これを回避するために予め対象を除外する機能もついているのですが，残念ながら警告を発する機能の方が優先度が高いため，結果として警告メールを発信してしまうケースがあります。

せっかく除外メールの設定ができるのですから，警告の優先度を高く設定するだけでなく，除外メールの優先度を高く設定できる機能なども加えられれば，より運用段階での実効精度が高まるのではないかと思います。

本誌　かなり贅沢な要望ですが，NetEvidenceという基本基盤があっての高度な要望だと思います。

米廣　それはその通りですね，ここまでできると，さらに次のレベルが欲しくなりますから（笑）。

ついでに言っておきますが，これはすぐに対応できないとは思いますが，SSLで暗号化された情報を検知できるようにして欲しいですね。社内で発行している暗号キーであれば，データの複合は不可能ではないわけですから，将来的にはSSL情報にも対応できるように機能強化を図っていただきたいと思います。

梅田　いただきましたユーザーからの要望は，必ずや将来のNetEvidenceをさらに向上させる源だと考えていますので，できる限り早い時期に実現し，更なる飛躍をとげていきたいと思います。

本誌　本日はありがとうございました。

株式会社インターメディアシステム
〒135-0042　東京都江東区木場1-5-25
深川ギャザリアタワーＳ棟10階
tel.03-3615-3441
http://www.intermediasystem.co.jp/

情報漏洩対策のフォレンジック製品　「NetEvidence」Ver.2.0がリリース

株式会社大林組（本社：東京都港区，脇村典夫社長）の情報子会社である株式会社オーク情報システム（本社：東京都墨田区，徳永正博社長）は，去る10月17日，同社の提供する情報漏洩対策製品「NetEvidence」のVer.２.０をリリースした。

「NetEvidence」は，ネットワーク経由で交わされる外部との通信データすべてを記録・保存することで，不正行為を抑止し，万一漏洩があった場合に漏洩者の特定と証拠保全に威力を発揮するフォレンジック製品。

2005年４月の個人情報保護法の施行などを背景に，自治体や企業は，ネットワークにおける情報セキュリティへの対応を本格的に始動させてきているが，「NetEvidence」もすでに多くの販売実績をもつ。

今回のバージョンアップは，同製品を導入し，先進的な取り組みをしているユーザーからの様々なリクエストを反映し，飛躍的にユーザーインターフェースの改良を図ったもの。

これと合わせて，サーバー本体のディスク容量も１.２TBまで拡張バックアップ装置に関する部分でも，従来のAIT３とLTO２に加えてO３（400GB）での対応が可能としている。

（株）オーク情報システムでは，今回のバージョンアップにより，コンピュータにそれほど詳しくない人でも容易に「NetEvidence」を操作することができるようになり，これまで情報システム部門に偏り勝ちであった情報セキュリティの運用が，監査や総務といった部門でも多面的に行えるようになると説明している。

なお「NetEvidence」では，ユーザーの規模等に応じて40種類以上のラインナップをそろえており，価格は220万円から1,000万円。

新たに加えられた高速検索エンジンやパケット取り出し機能などのオプションも豊富で，それぞれのユーザー環境にあった最適な構成を選択することができる。

NetEvidence新バージョン（Ｖ２）の特徴（Ｖ１との相違点）は次の通り。

①利用者IDの複数化を実現
②利用者IDごとの利用権限の限定化
③利用者操作画面の変更
④Web検索条件の追加
⑤Web閲覧画面の再構成表示内容の変更
⑥利用者情報のログ出力機能の追加
http://www.oakis.co.jp/NetEvidence

株式会社オーク情報システム
（大林組グループ）
〒131-0034　東京都墨田区堤通1-19-9
リバーサイド墨田セントラルタワー
tel.03-5247-3200/fax.03-5247-3231
http://www.oakis.co.jp