



セレクト

2.0

ビジネスイノベーターのためのIT活用情報誌

新 企業防衛論

D i g i t a l F o r e n s i c

デジタル・フォレンジック時代 到来！

●デジタル・フォレンジックとは？

インシデント・レスポンス<コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為(事象)等への対応等を言う>や法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術をいう。

上記は、特定非営利活動法人デジタル・フォレンジック研究会による、「デジタル・フォレンジック」の定義だ。デジタル・フォレンジックは米国を中心に世界各国で犯罪捜査や裁判の場などで広く使われており、企業でも内部不正対策の一つとして広まりつつある。また、デジタル・フォレンジックに使われる各種システム(フォレンジック・ツール)も、すでに数多く登場している。こうした動向を受けて、日本でもデジタル・フォレンジックが注目され始めた。訴訟対策、企業の社会的責任(CSR)、さらに内部の不正発見・追求、不正抑止や従業員保護といった観点から、企業とデジタル・フォレンジックの深い関わりを紹介する。

シーア・インサイト・セキュリティ
代表取締役 CEO
向井 徹 氏



デジタル・フォレンジックは 企業や経営者にとって重要

普段は見えない情報から
証拠を見付け出す技術

日本における活用は
まだこれから

コンピュータの中には、普段ユーザーの目に触れることのない大量の情報がある。そういった情報を収集・分析し、犯罪捜査や裁判の証拠として用いることがしばしば行われるようになってきた。そのため技術・手法がデジタル・フォレンジックである。

デジタル・フォレンジックは大きく「コンピュータ・フォレンジック」「ネットワーク・フォレンジック」の二つに分けられる。前者はハイテク犯罪捜査や企業のインシデント・レスポンス、後者は情報セキュリティマネジメントをカバーする。

企業において、デジタル・フォレンジックは訴訟対策や情報セキュリティ課題への対策として用いられる。例えば個人情報情報漏えい対策としてであれば、情報漏えい発生時の漏えいルートやプロセスの把握、あるいは疑わしいユーザー挙動の確認をコンピュータ・フォレンジックで行い、ネットワーク・フォレンジックは漏えい防止を目的とした監視基盤や、漏えい発覚時の情報源となる。

日本では、まだデジタル・フォレンジックがあまり普及していない。認知度そのものも低いというのが実情だ。近年になって個人情報漏えい事件が頻発し、2005年4月に個人情報保護法（個人情報保護に関する法律）が完全施行されたことで、ようやく情報漏えい対策の一環として一部の企業でデジタル・フォレンジックが使われ始めた。例えば、個人情報漏えい事件を起した企業が「詳しい流出経路は不明」しかコメントできないようでは、ただでさえ失墜した社会的信用をさらに下げるばかり。そこに気付いた企業が、デジタル・フォレンジックによって対策を始めている。

それを受けて、デジタル・フォレンジック関連企業の活動も活発化しつつある。コンピュータ・フォレンジックのコンサルティングや関連ツールの輸入・販売、およびコンピュータ・フォレンジック技術者を育成するトレーニングを手掛けるUBICは、5月に日本で唯一の「コンピュータ・フォレンジックラボ」を設立、企業や公共団体向

けのアウトソーシングサービス
を本格的に展開し始めた。

同社代表取締役社長の守本正宏氏は、大企業を中心に多くの企業がデジタル・フォレンジックに注目しており、これから普及に弾みがつくという見通しを示している。

「これまで、日本にはフォレンジック・エキスパートがほとんど存在しませんでした。しかし、情報漏えいのインシデント・レスポンスや海外での訴訟対応には、デジタル・フォレンジックの知識を持った人材が不可欠となっています。今後、企業にとってデジタル・フォレンジックの重要性はますます増大してくるでしょう。そのニーズに応えるためには、企業に代わってコンピュータ・フォレンジック調査を提供するアウトソーシングサービスや、日本国内でのフォレンジック・エキスパート育成が必要となるのです」

日本では、コンピュータ・フォレンジックよりネットワーク・フォレンジックの方が普及は進んでいるようだ。

「我々が調べたところ、ネットワーク・フォレンジックの中でも電子メールの管理・保全は普及が進んでおり、調査対象のうち約60%の企業が実施しています。それに次いで、約50%がファイアウォールや各種サーバーのログ、クライアント操作ログなどの管理を行っています。操作ログなどの監査は、個人情報保護法ガイドラインでも求められていますから、だいぶ対策が進んできたと言えるでしょう」と語るのは、シーア・インサイト・セキュリティ代表取締役CEOの向井徹氏。同社はネットワーク・フォレンジック関連ツールのベンダーだ。

「UBICとシーア・インサイト・セキュリティは、7月にフォレンジック・サービスに関する業務提携を行った。その背景には、コンピュータ・フォレンジックとネットワーク・フォレンジックの両輪であり、相互の協力が欠かせないという認識があるようだ。」

二つのフォレンジックが
より確実な結果をもたらす

「コンピュータ・フォレンジックの調査には時間がかかります。1000台、1万台ものクライアントを全数調査するなど、まず不可能です。まず、ネットワーク・フォレンジックで疑わしい端末を絞り込む必要があります」とUBICの守本氏は言う。

また、確実性を高めるために

デジタル・フォレンジックの 技術

証拠探しの技術



UBIC
代表取締役社長
守本正宏 氏

コンピュータ上のデータ消去は、実は完全消去ではない。ファイル操作を迅速に行うため、通常はデータの所在を示す情報をファイルシステム上から消去しているだけで、実際のデータそのものは上書きされるまでそのまま残っている。またOSには様々な記録（ウィンドウズの「レジストリ」など）が残されており、これらを解析することで過去の利用状況を明らかにすることが可能だ。

デジタル・フォレンジックにおいては、これらの原理を利用して残されたデータを復元し、証拠を探す技術が含まれている。本特集では、そうした証拠探しの技術・手法を「コンピュータ・フォレンジック」と呼ぶことにする。

コンピュータ・フォレンジックは、主に犯罪捜査や、何らかの事後対応（インシデント・レスポンス）として用いられる。例えば社内のPCから個人情報が入り込んだ場合、その漏えいがどのようなルートで、どのようなプロセスを経て行われたかを、コンピュータ・フォレンジックによって明らかにすることができる。

具体的には、まず、漏えい元とされるPCからHDDを取り出し、その内容を別のHDDにコピーする作業が行われる。これは複数手段の解析を同時に並行して行うため、また解析時のミスなどでオリジナルデータに改変を加えてしまった場合のバックアップが目的だ。その際、ファイルシステムに残っていないデータも完全にコピーするため、専用のコピーツールを用いる必要がある。コピー先のHDDについても、余計なデータが紛れ込むことのないよう、あらかじめ完全なデータ消去を行っておくことが重要だ。

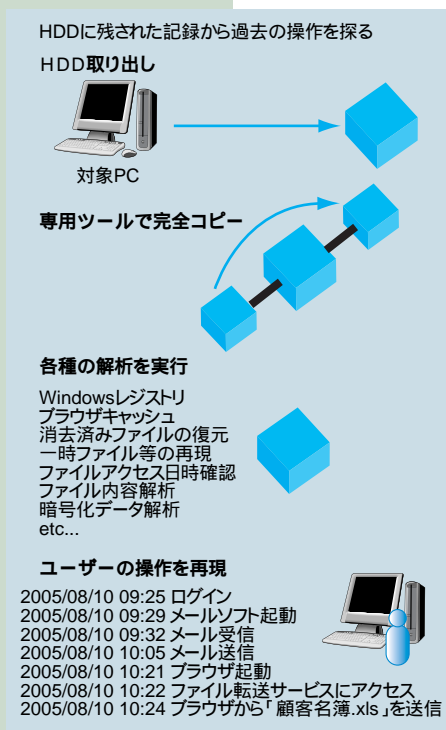
コピーされたHDDの中身を解析するには、複数のツールが用いられる。例えば、ウェブメール経由で漏えいしたのなら、ブラウザの過去のアクセス先やキャッシュから送信内容を調べることで判断できる。USBメモリなどから持ち出されたのであれば、外部記憶媒体への書き込みの際に作られる一時ファイルが見つかるはずだ。それらのファイルが暗号化されている場合でも、暗号解析ツールを使って中身を確認できる。それぞれの解析内容を総合して、ユーザーのPC操作を再現することも可能だ。

も、両方のフォレンジックが重要となる。コンピュータ・フォレンジックを使えば消去されたファイルの内容も判別できるが、消去後の時間の経過に伴い、その残存データが上書きされるなどして残存率は低下していく。また、廃棄済みPCからの情報流出を防ぐ目的で「完全消去ツール」が出回っているが、これらはランダムなデータを何度も上書きするなどして、データ復元も防ぐというものだ。「完全消去」された状態からでも、実験室レベルでなら過去の記録内容を

を復元できるとされているが、実用的な時間・コストで調べられる範囲はどうしても限られるのが実情だ。事件発覚後、あるいは告発があつてから調べても、手遅れになる可能性がある。ネットワーク・フォレンジックを活用して定期的な監査や疑わしい行為の監視を行い、より早い段階でコンピュータ・フォレンジック調査を行うことが望ましいのだ。

実際、コンピュータ・フォレンジックとネットワーク・フォレンジックを組み合わせて、総合的なデジタル・フォレンジック体制を運用している日本企業があると向井氏は言う。「我々を知る限り、まだ1社のみ。名前は明かせませんが、万単位のクライアントを擁する大企業です。その会社では、ネットワーク・フォレンジックによる定期監査で、疑わしい行為

が月に数件は見つかるそうです。それを詳しく調べるにはログだけでは限界があるので、コンピュータ・フォレンジックの調査を行うという体制です。今後は、金融系などセキュリティに厳しい業種を中心として、このような総合的フォレンジック体制が広まると思います」



宇都宮大学 工学部 講師
弁護士
高橋郁夫 氏



デジタル・フォレンジックと企業、そして従業員の間にあるもの

デジタル・フォレンジックは経営者が理解しておくべき

一方、デジタル・フォレンジック先進国である米国では、多くの企業がデジタル・フォレンジックに取り組んでいる。

宇都宮大学 工学部 講師で弁護士の高橋郁夫氏は、米国フォレンジック事情の視察でプリンガム・ヤング大学（BYU）を訪れ、フォレンジック・コースについての説明を受けた。

「米国でも、企業統治の観点でデジタル・フォレンジックに注目が集まっています。これからの経営者はデジタル・フォレンジックについての理解が必要だ、という考えもあるようです。BYUは、会計学と合わせて会計に関連したセキュリティの教育を行っているとのこと。まだ数は少ないものの、フォレンジックの講座を持つ大学が他にもいくつかあるそうです」

監視対象となる従業員のプライバシーという問題

なお、高橋弁護士は、ネットワーク・フォレンジックによる監視や監査について、行き過ぎがないようにと警鐘を鳴らして

いる。

「最近では、性悪説の時代だということになって、企業が従業員を監視するのが当然だという風潮になってきている。しかし、企業秩序を重視するあまり、従業員のプライバシーをないがしろにするほどの監視を行うのは法的な問題になりかねません。企業マネジメントの観点からも、従業員がモチベーションをなくすほどの厳しい監視／監査体制は望ましくありません」

プライバシー保護であるはずの社内監視が従業員のプライバシー侵害になりかねないというのは、皮肉な問題と言える。上手にバランスを取る必要があります。

こうした課題に対し、以前から従業員の活動をモニタリングしている企業では、どのような取り組みを行っているのだろうか。ヒューレット・パカード（以下HP）では、個人情報保護のためのモニタリングを行う中で、様々なルールを決めているという。

日本HP 個人情報保護対策室 室長の佐藤浩氏は「広い意味でのモニタリングとしては、情報の取得から最終的な判断まで、図のような流れになっています。

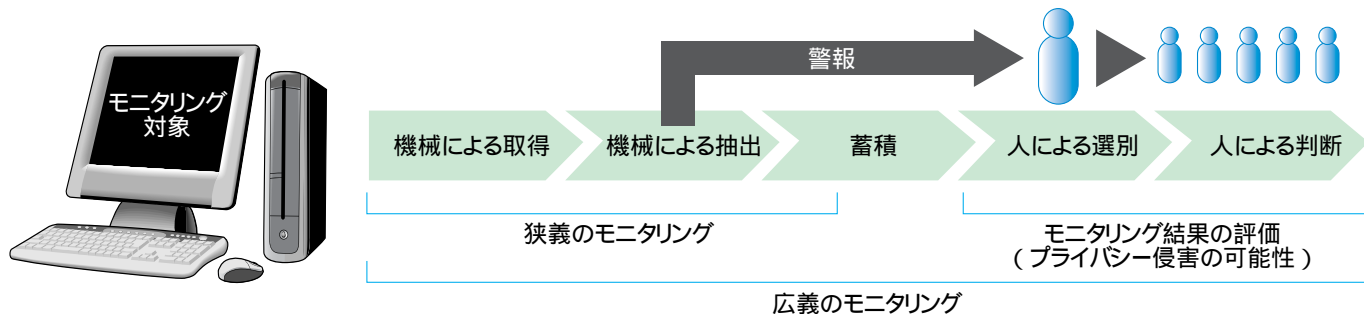
このうち、蓄積までの狭義のモニタリングの段階においては、機械的に行われるものです。機械に人格権はありませんから、プライバシー侵害に相当しないと考えています。一方、人間による評価を行う際にはプライバシー侵害の可能性が出てきます」と語る。

機械的監視の結果、何らかのアラートが出たりすれば、人の目で蓄積された情報の選別を行ったり、選別された情報を元に問題行為かどうか判断することになる。

「そもそも当社では、従業員のプライバシーに相当するような部分の情報は、蓄積対象からほとんど除外されています。そして、モニタリング結果の判断に際しては、判断対象人物を直接知っている者が参加すべきではないというルールになっています」（日本HP・佐藤氏）

対象を知らない人物が判断すること、公平な視点を得ようとする工夫である。見知らぬ相手、公平な判断が期待できるなら、プライバシーへの期待もできそうだ。しかし、誰もが顔見知りであるような小規模企業では、このような対処はまず不可能。第三者の視点を得るため、

広義のモニタリングの中で、人が関与する部分では従業員プライバシー侵害の可能性がある(日本HP・佐藤氏提供)



デジタル・フォレンジックの 技術

証拠保全の技術

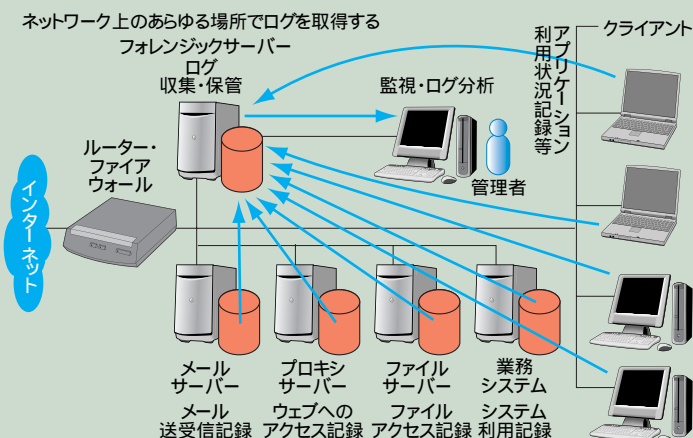
デジタル・フォレンジックでは、紛争の事前対策や不正行為の抑止力として、各種の記録を取得・保存して証拠とすることも含まれる。また、記録取得の際にリアルタイム監視を併用することで、より強い抑止力を働かせることができる。これらの証拠保全技術・手法は主にネットワークの利用記録が中心であることから、本特集では「ネットワーク・フォレンジック」と呼ぶことにする。

事前対策において、比較的広く行われているのが電子メールの保存だ。メールサーバーを通った全てのメール（送信/受信の両方）を専用の領域に一定期間保存しておけば、クライアント側でメールを消去してしまっても、外部とのやり取りを再現することができる。同様に、業務システムへのログイン記録やアクセス記録、ファイルサーバー上のファイルアクセス記録といった情報を残しておけば、業務外の利用が行われたかどうかを確認できる。

さらに、より詳しい情報を記録するため、ネットワーク上を流れるデータを全て記録しておく手段もある。ただし、この方法では、保管すべきデータ量が非常に多くなるため、あまり広く普及してはいないようだ。

また、クライアントからの情報漏えい事件が増加してきたことに対応し、最近では各クライアントでのファイルアクセス記録、アプリケーション利用状況記録などを収集しておくことも行われるようになってきた。

こういった各種の手法で収集されたログは、改ざんを受けたり消去されたりしないよう、専用の高いセキュリティを持つサーバーに保管される。そのログを定期的に分析することで利用状況を確認できるほか、収集と同時に特定の条件で警告を出すなどの対応も可能となり、不正行為を行わないよう監視することもできる。



日本コンピュータ・ネットワーク
個人情報保護対策室
室長
佐藤慶浩 氏

社外に監査を委託することも必要になるだろう。

「大切なのは従業員と企業の信頼関係です」と佐藤氏は言う。信頼されていないと感じれば監視や監査が苦痛となる。それは絶対に避けるべきだ。

「フォレンジックは犯人探しの手段ではありませんし、監査は最終兵器と考えた方が良いでしょう。よほどのことがなければボタンを押せませんが、抑止力として役に立つのです。そして企業は、『従業員の潔白を証明するためにこそモニタリングを

行っている」という姿勢を明確にすべきでしょう」

日本企業にとっての 今そこにある危機

日本企業のデジタル・フォレンジックへの対応の遅れが、密かに大きな問題となっている。米国の裁判では、米国の手法に合わせて証拠提出を行う必要がある。もちろん日本企業も例外ではないが、電子データを求められた場合には、米国の電子データ開示手続き（eディスカバ

リ）に沿って提出せねばならない。

高橋弁護士は「民事訴訟での訴え方の思想が日本と米国とで大きく違っており、特に電子データを証拠とする場合には、その扱い方や手続きなどが全く異なります」と説明している。そこに、日本企業がつけ入られることもあるという。

UBICのコンピュータ・フォレンジックラボは、視察に訪れた米国の弁護士から「米国の訴訟に対応できる、日本で唯一の施設」と評価された。言い換

えれば、日本にはそういった施設がまだ一つしかなく、5月の設立までは全く存在しなかったということになる。

UBICの守本氏は言う。

「米国の訴訟で証拠として経営層のデータを求められ、eディスカバリの手順に従って従業員の端末からHDDを取り出して提出させられた、というケースは少なくないようです」

そのHDDが、どのように扱われるかは相手次第。証拠を探すという名目で、他のデータも一緒に抜き出している可能性だ

デジタル・フォレンジックの将来像

ってある。だが、部分的にデータを取り出して提出するにも、「他のデータは提出の必要なし」と主張するにも、eデイスカバリに準拠せねばならない。このままでは日本企業がカモにされてしまう危険があると守本氏は

警告する。

「すでに多くの企業が切迫した状況にあるか、実際に不利益を被っていると思われる。当社への相談も相当な数に上ります」

最大の課題は、日本人フォレンジック・エキスパートが少な

いこと。米国人のフォレンジック・エキスパートに依頼しても、日本語が分からなければ提出の必要があるのかないのかを判断することは難しい。だがeデイスカバリに対応できる知識やスキルを持ち、かつ日本語に堪能

で、日本企業の実情に明るい人材は、まだほとんどいない。「まさに、今そこにある危機」という状況です」（高橋弁護士）
日本でのフォレンジック・エキスパート育成は、急務と言えるだろう。

デジタル・フォレンジックにまつわる日米法曹界の相違点は、どのように解決されていくのか。そして、日本企業は、どのようにデジタル・フォレンジックへ取り組むべきなのか。慶應義塾大学 大学院法務研究科 法学部教授で、特定非営利活動法人デジタル・フォレンジック研究会 副会長を務める安富潔弁護士に聞いた。

日米で食い違う裁判基準にいかに対応していくか

——犯罪捜査や裁判における日本のデジタル・フォレンジック対応状況は？

安富 まず、警察の捜査活動の中では、ハイテク犯罪捜査を中心に、刑事事件の証拠収集手段としてデジタル・フォレンジックが活用されています。

現在の日本では、警察が最も充実したデジタル・フォレンジック組織を持っていると言えるでしょう。警察では、ハイテク犯罪だけでなく、例えばオウム真理教事件などの重大事件にデジタル・フォレンジックを活用し、重要な証拠を見付け出しています。最近の事件でも、「自殺

サイト殺人事件」で容疑者が犯行の直前に「もう死ぬのだからメールは消してください」と被害者に指示したというニュースがありましたね。この場合も、「メールが存在した」という証拠

を被害者のPCから見付け出すためにデジタル・フォレンジックが役立つことでしょう。

一方、民事事件に関しては、刑事事件と違って証拠能力に関する制約がないことから、「使える証拠はどんどん使う」という

スタンスで扱われます。ですから、電子データに証拠力があるかどうかという問題に尽きてしまい、今まであまり議論されてきませんでした。

日本の法曹界では、まだデジタル・フォレンジックが正式に

認知されている状況ではないですね。

——国際的なデジタル・フォレンジックの標準化動向について教えてください。

安富 日本企業が米国で訴えられたとき、米国裁判基準に合わせた対応が必要だという課題があります。その根幹には、証拠に対する考え方、そして証拠の使い方が異なるという、日米間の相違があります。

日本の法制度では、証拠提出命令を受けて提出するのは、例えばプリントアウトした紙資料で良いのです。目に見えないデータを証拠とするような文化がないから、物理的な形で持つてくるわけです。

それに対し米国は、「eデイス

カバリ」と呼ばれる電子的な証拠提出手順があります。媒体はフロッピーデイスクでもCD・RでもHDDでも構いませんが、データそのものを持つてくる必要があります。つまり情報そのものが証拠として求められているのです。

分かりやすく言えば、あなたがメモしているその取材メモが仮に証拠として求められたとすれば、日本なら「ノートそのものを」求められるでしょう。米国ならば「ノートに記載されている内容を」求められますが、その媒体はコピーでもワープロ文書でも構わない。

このように、証拠に対する考え方が根幹から違っていますから、日本が米国のような考え方を



になるには、コペルニクスの転回がなければ難しいかもしれませんが。

ですが、おそらく日本でも、必要に応じてデータそのものを証拠とするような動きも出てくるでしょう。そうなった場合でも、証拠として求めるのが媒体そのものか、それとも情報かというのは、立証しようとする対象によって使い分けられることになると思います。何でもかんでも米国的に、情報の提出を求めるようになるわけではないでしょう。

証拠としては、もちろん原本

が最良です。だけど原本がなければ写してもいい。もちろん、その写しは原本と同一でなければなりません。デジタル情報は変わりやすいものですから、写しのプロセスをきちんと整えて、裁判官に理解できるようにしておくことが必要となります。

企業にとって「攻め」のセキュリティ

——特定非営利活動法人デジタル・フォレンジック研究会では、デジタル・フォレンジックの認知度向上について取り組んでい

ますが、日本企業におけるデジタル・フォレンジックの浸透はどの程度まで進んでいるのでしょうか？

安富 日本企業におけるデジタル・フォレンジックの認知度は、まだ低いと思います。ようやく少し認知されてきたかな、という程度でしょう。

企業において、デジタル・フォレンジックは、企業活動の正当性を証明する手段、例えば株主から何らかの不正を疑われたときなどに、その不正が実際に行われたのか、行われたのなら具体的にどのようなプロセスを経てのものなのか、といった情報を提示するのに役立ちます。例えば、「カネボウ粉飾決算事件」でも、会計の不正操作を行う過程でいろいろな計算をしているはずですから、デジタル・フォレンジックによって責任を明確化することができます。

近年、経営者の責任を明確に規定する制度が増えてきました。ご存知の通り米国ではSOX法(Sarbanes-Oxley Act)が施行されていますし、日本でも商法などの改正が行われています。社会的な風潮としても、コンプライアンス、経営健全性、内部統制などが求められており、経営者は説明責任を果たす必要があります。そうした中、今後は経営者が自分たちの行為の正当さを示すために、デジタル・フ

ォレンジックを活用することが不可欠になってくると思われる。

米国では「CFE」(Certified Fraud Examiner: 公認不正検査士)という資格認定制度があって、多くの企業で企業活動の正当性の証拠を作るなど活躍しています。日本企業の中でも、米国でCFEを取得してきた方が活躍しているケースが増えてきました。この資格は米国の公認不正検査士協会(The Association of Certified Fraud Examiners: 略称ACFE)が認定するもので、日本にもACFEの支部が設立されて動き出しています。今後、より多くの企業で、会計士や監査人のように、不正検査士が活動することになっていくことでしょう。

——デジタル・フォレンジックで、企業の活動も大きく変わってくるのですね。

安富 私見ですが、従前、企業にとつてのセキュリティといえば「守り」のイメージでした。しかし、広い意味で、セキュリティには「守り」と「攻め」の両面があると思います。その「攻め」に相当するのが、自分たちが積極的に一つひとつ証拠を残しつつ活動する、デジタル・フォレンジックだと思っております。「守り」というイメージが強いセキュリティの考え方を変えていくものが、デジタル・フォレンジックだと言えるでしょう。■



シーア・インサイト・セキュリティ株式会社

〒108-0023 東京都港区芝浦3-14-8芝浦ワンハンドレッドビル3F

e-mail: info@seerinsight.co.jp

<http://www.seerinsight.co.jp/>



株式会社 UBIC

〒108-0075 東京都港区港南2-12-23 明産高浜ビル7階

e-mail: sales@ubic.co.jp

<http://www.ubic.co.jp/>