2017 年 6 月 1 日
株式会社フォーカスシステムズ
日本マイクロソフト株式会社

サイバー犯罪の証拠データ分析の高速処理化に向け、フォーカスシステムズと日本マイクロソフトが連携

Microsoft Azure を活用したソリューションにより、分析時間を3日から半日に短縮

株式会社フォーカスシステムズ（本社：東京都品川区、代表取締役社長：森啓一、以下フォーカスシステムズ）と日本マイクロソフト株式会社（本社：東京都港区、代表取締役 社長：平野拓也、以下日本マイクロソフト）は、サイバー犯罪の証拠データの分析及び鑑識（サイバーフォレンジック）の高速処理化に向けて連携します。本連携により、マイクロソフトのクラウドプラットフォーム「Microsoft Azure（以下Azure）」を活用した警察機関向け証拠データの高速処理化を実現するソリューション「サイフォクラウド」を本日より提供開始します。

サイバー犯罪の証拠データの分析及び鑑識作業の分野においては、PCやスマートフォンなど、様々なデバイスの解析作業のために事前のデータ処理作業（データカービングやインデックス、圧縮ファイルの展開、ハッシュ計算等）が必要となります。現状では、そのデータ処理に膨大な時間が必要で、平均して約3日の作業時間が掛かることが、サイバー犯罪捜査の検挙への大きな課題となっています。さらには、データの大容量化、解析対象となるデバイス自体の増加など、今後もますます証拠データの分析及び鑑識作業のニーズは増す一方で、事案に対する時間的な制約や、人的、物的なリソース不足も発生しています。
このような状況の中、分散処理技術やパスワード解析技術をはじめとしたフォーカスシステムズのサイバーフォレンジックソリューションと、マイクロソフトのクラウドプラットフォーム Azure を連携させる実証試験を実施しました。実証試験の結果により、従来の分析時間を3日から半日に短縮（※）する結果となりました。1日以内の分析を実現することにより、サイバー犯罪の検挙へ大きく貢献できるソリューション「サイフォクラウド」が誕生しました。

本日より全国の警察機関、並びに法執行機関向けにサイバーフォレンジックソリューション「サイフォクラウド」をフォーカスシステムズから提供開始します。日本マイクロソフトはフォーカスシステムズと連携し、全国の警察機関、並びに法執行機関に向けて、本ソリューションの提案サポートと技術支援を行います。

フォーカスシステムズと日本マイクロソフトは、サイバー犯罪の証拠データの分析及び鑑識作業のさらなる高速処理化に向けて連携し、警察機関と法執行機関のデジタルトランスフォーメーションの推進を支援いたします。

※実証試験において、一般的なケースとして１TBの下処理作業の場合、従来約3日を要していたものが、半日程度に短縮できる結果となりました。

◇

「サイフォクラウド」概要

ソリューション名	サイフォクラウド
提供開始日	2017年6月1日
概要	警察機関向け証拠データの処理作業の高速化を実現するソリューションです。 サイバー犯罪の証拠データの分析及び鑑識（サイバーフォレンジック）作業を行うためには、消去されたファイルの復元や、検索、分析処理を行うためのデータのインデックス作成など、事前に下処理作業を行う必要があります。 従来、利用するソフトウェアの制約などから、ワークステーションなどのスタンドアロンの端末を用い、下処理作業を行うことが多く、下処理作業が完了し、担当者が、分析及び鑑識作業が行えるようになるまでには、多大な時間を要していました。また、分析及び鑑識作業をはじめると、パスワードがかかったファイルなどは解析できるようになるまでに、さらに時間を要することもあり、お客様の生産性に大きな制約を強いています。 本ソリューションでは、フォーカスシステムズの分散処理技術を利用し、下処理作業やパスワード解析作業を Azure 上のコンピューターノードで並列分散処理させることで、処理を倍速化させます。また、クラウド基盤を利用することで、これまで、作業を開始するとコンピューターリソースの占有が必要となり、空きのコンピューターリソースが用意できない場合には、他の事案に対する待ち時間が発生した点や、下処理を終えたい時間があってもコンピューターのスペックなどに制約を受けた点が、オンデマンドにコンピューターリソースを利用できるようになり、捜査員の生産性の向上に大きく寄与します。

実証試験に関して

実証試験名称	フォレンジックソフトウェアの並列分散処理に係る高速化実証試験「MSA-ADPASS」
期間	2017年2月１日（水）～3月24日（金）
概要	警察機関向け証拠データの処理作業の、クラウド環境における高速化に関する実証試験です。 警察機関向け証拠データの下処理作業について、フォーカスシステムズの分散処理技術および Azure によるクラウド環境を用いて高速化の試験を行いました。システム構成については、Azure のAシリーズを用い、認証用サーバー、データベースサーバー、ファイルサーバーの構築を行うとともに、下処理作業を分散させるエンジン用サーバーで構成されています。

	実証試験においては、下処理作業分散エンジンを1台での単独処理、3台および4台での分散処理の計3ケースにおいて、正常に処理がなされた上で、処理スピードの高速化が図れるか、どの程度の高速化が図れるかという点の確認を行いました。
結果	実証試験の結果、CPUのコア数に比例してデータ処理作業の高速化を実現できることを確認しました。 従来、1台のサーバーを用いて、50GBのデータに対し下処理作業を行った場合、約3時間の処理の時間を要していました。この50GBは、一般的な使用ケースとしては、１TBの下処理作業となります。１TBの想定で、1台での単独処理の場合、実際の分析及び鑑識作業が行えるようになるまでに約3日必要ということです。 今回、分散エンジンを4台で処理させることにより、この１TBの下処理作業で約3日要していた処理が、半日程度で分析及び鑑識作業が開始できるようになる結果となりました。なお、下処理用の分散エンジンをさらに複数台配置させることで、さらなる処理の高速化を図ることも可能であり、警察機関の生産性に寄与するとともに、捜査プロセス全体に大きな影響を与えることが可能なソリューションであることを確認しました。
結果詳細	https://cyberforensic.focus-s.com/

◇

【フォーカスシステムズについて】

フォーカスシステムズは、2004年からフォレンジック事業に参入しており、官公庁や法執行機関はもちろん、多くの民間企業に実績を持っております。当社の製品およびプロフェッショナルサービスは、従来のデジタルフォレンジックからサイバーセキュリティまでカバーしており、これまで培ってきたノウハウを活かしたリスクマネジメントコンサルティングをお客様にご提供しております。

【日本マイクロソフト株式会社について】

日本マイクロソフトは、マイクロソフト コーポレーションの日本法人です。マイクロソフトは、モバイル ファースト& クラウド ファーストの世界におけるプラットフォームとプロダクティビティのリーディングカンパニーで、「Empower every person and every organization on the planet to achieve more.（地球上のすべての個人とすべての組織が、より多くのことを達成できるようにする）」を企業ミッションとしています。
日本マイクロソフトは、この企業ミッションに基づき、「革新的で、安心でき、喜んで使っていただけるクラウドとデバイスを提供する会社」を目指します。

この件に関する報道関係の方からのお問い合わせ

株式会社フォーカスシステムズ

担　当：　サイバーフォレンジックセンター　池田
電　話：　03-5421-7360（部門代表）
Fax：　03-5449-9051
E-mail：　forensic@focus-s.com
ホームページ：　https://cyberforensic.focus-s.com/
https://www.focus-s.com/（コーポレートサイト）
住所：　〒141-0022　東京都品川区東五反田 1-14-10 三井住友銀行五反田ビル 7 階

日本マイクロソフト株式会社

担　当：　コーポレートコミュニケーション本部　巽
電　話：　03-4535-8055（部門代表）
Fax：　03-3472-7853
E-mail：　mskkpr@microsoft.com
公式 Twitter：　@mskkpr
公式ブログ：　http://blogs.technet.com/b/microsoft_japan_corporate_blog
Facebook：　http://www.facebook.com/microsoftjp
住　所：　〒108-0075　東京都港区港南 2-16-3 品川グランドセントラルタワー