SAP ジャパン

SAP HANA の最新版を提供開始

SAP ジャパンは、SAP HANA プラットフォーム向けサービスパック 10（SPS10）の提供を開始した。SAP の CTO（最高技術責任者）であるクエンティン・クラーク氏は、「SAP HANA は、トランザクションと分析処理を 1 つの統合プラットフォームで実行します。SAP HANA の今回の新機能により、データセンターの正常稼動とすべてのリモートシステムへのデータ同期を確実に行い、エンタープライズデータの高可用性と耐障害性を強化し、高度な分析を実施することができます。これによりお客様は、経済全体のデジタル化という避けることのできない流れに備えることができます」と語っている。

◆ Internet of Things とエンタープライズレベルで接続：企業は、SAP HANA の新しいリモートデータ同期機能により、エンタープライズとネットワーク末端のリモートロケーション間でデータを同期することができる。1,200 万超のライセンス実績を有する先進のエンタープライズ対応埋め込み型データベーステクノロジー SAP SQL Anywhere スイートを利用して、エンタープライズとリモートロケーション間で SAP HANA リモートデータ同期を実行する IoT（Internet of Things）およびデータ集約型モバイルアプリケーションを開発できるようにもなった。

◆ビッグデータのデータアクセスと管理を合理化：企業は、SAP HANA の拡張されたスマート・データ・インテグレーション機能により、Cloudera や Hortonworks、MapR といった最新の Hadoop ディストリビューションを導入して、ビッグデータを継続的に利用できる。SAP HANA の追加拡張機能には、Spark SQL による高速データ転送、SAP HANA および Hadoop のクラスター管理を、Apache Ambari を利用することで、単一ユーザーインタフェース（UI）で行うことができる。

◆企業全体にわたる高可用性とスケーラビリティの強化：SAP HANA は、高可用性と耐障害性の新しい機能によって、データセンターの正常稼動を確保し、常時オンのミッション・クリティカル・アプリケーションへの対応を支援する。1 対 n の非同期レプリケーション、ダイナミックティアリングの自動ホストフェイルオーバー、増分バックアップなどの機能は、システムのダウンタイムを短縮し、企業全体にわたって真の事業継続性を促進するのに役立つ。

◆高度な分析によるイノベーション：SAP HANA SPS10 の拡張されたデータ処理機能を利用すれば、高度な分析機能を備えた強力なアプリケーションの開発を加速できる。また、SAP HANA のテキストマイニングが SQL 構文にまで拡張され、次世代アプリケーションを開発しやすくなった。

◆大きな弾みがつく SAP HANA：SAP HANA を利用してビジネスを変革するお客様の数が劇的に増大している。SAP HANA のお客様は、現在 6,400 社を超え、わずか 1 年の間にほぼ倍増した。SAP HANA Cloud Platform も、短期間でおよそ 1,400 社に導入されるという勢いだ。2015 年だけでも 370 社を超えるお客様が SAP Business Suite 4 SAP HANA（SAP S/4HANA）を利用して、すぐに巨大な利益を生み出した。SAP HANA 上の SAP Business Warehouse アプリケーションは、1,900 社を超えるお客様から引き続き強力な支持を得ている。新興企業による SAP HANA の導入件数も急上昇し、現在では、2,000 社を超えるユーザーが SAP HANA プラットフォームを活用している。

● SAP ジャパン
TEL：0120-786-727

NEWS

ファイア・アイ

セキュリティ侵害の発生からの復旧を目指す 国内向けのセキュリティ・アズ・ア・サービス「FireEye as a Service」を発表

高度なサイバー攻撃の対策製品・サービスで業界をリードするファイア・アイは、同社のテクノロジーと脅威情報、専門知識を活用し、高度なサイバー攻撃による被害を最小限にとどめる新たなセキュティサービス「FireEye as a Service（ファイア・アイ・アズ・ア・サービス）」を、2015年内にセキュリティパートナーと協業して国内で提供を開始することを発表した。

FireEye as a Serviceは、高度なサイバー攻撃の事前予防的な検知から、万一セキュリティ侵害が起きた際の迅速な対応を支援し、復旧にかかる時間の大幅な短縮を可能にする監視・解析を提供するサービスだ。ファイア・アイ調べの最新調査によると、現在、企業や組織において、高度なサイバー攻撃が行われ、それが発見されるまで平均205日かかっている。また、実に69%の企業、組織はその事実に外部から指摘されるまで気づかないことが明らかになっている。ファイア・アイでは、最近の高度なサイバー攻撃は検知テクノロジーだけで対処するのは困難になっているという前提で、国や業種、その他お客様の環境ごとの固有な情報に基づく脅威情報に照らした事前予防的な解析を定期的に実施し、セキュリティ侵害に備える「適応型防御（Adaptive Defense）」の考え方に基づいたセキュリティソリューションを提供している。その中で、FireEye as a Serviceは、きわめて専門的な知識が求められる高度なサイバー攻撃対策をサービスという形でお客様に提供する新たなソリューションとなるものだ。

FireEye as a Serviceは、ファイア・アイのテクノロジー、脅威情報、専門知識をお客様に提供することで、従来型のアプローチと比較して10分の1の時間でセキュリティ侵害を検知、防御、解析、解決することが可能なサービスだ。同サービスの特長は、以下のとおり。

◆強力な防御機能：ファイア・アイがグローバルで収集・解析した最新の脅威情報を60分毎にお客様環境に配信し、強力な検知および防御の仕組みを実現する。

◆ファイア・アイの専門家による高度な脅威に対する監視と調査：ファイア・アイの脅威専門解析チームが24時間365日体制でお客様のネットワークとエンドポイントを監視し、セキュリティ侵害の兆候を見つけ出す。侵害の痕跡が発覚した場合は、問題のシステムに対して詳細な解析を実施し、それが本当に攻撃につながる脅威かどうかを確認する。

◆セキュリティ専任者でなくとも分かりやすい「具体的な対策」を提示：実際のシステムやネットワークのフォレンジック・データを利用して、リスクの調査、分類、解析をリアルタイムで実施。その後、実際に発生している事案に関する情報と、被害を抑止するために推奨される対策をまとめた詳細なレポートを1時間以内に送付する。

◆問題のホストを迅速に隔離：情報流出や攻撃・感染拡大などのリスクが切迫している場合、企業ネットワークに接続しているかどうかを問わず、問題のホストを直ちに隔離する。

◆インシデント対応：セキュリティ侵害が起こった場合、専門のインシデント対応担当者が素早く侵害状況を調査し、ネットワークのセキュリティ強化と技術的な被害の回復を実施。また、ビジネスへの影響を評価して、正確で速やかな情報開示を支援する。

◆継続的な改善：お客様毎のリスクに焦点を当てたセキュリティ脅威のプロファイル情報を提供。お客様や同業他社を狙っている攻撃者の特徴、手法、目的などを把握することにより、将来的な攻撃への対策や対応能力を強化できる。

●ファイア・アイ
TEL：03-4577-4432

びじねす玉手箱

NEC

セーフティ事業のグローバルなソリューション開発を加速する「顔認証技術開発センター」を設置

NECは、社会価値創造を実現する事業の一つとして、「セーフティ事業」を推進している。その中で世界トップレベルの認証精度を有する顔認証技術は中核となる先進技術だ。本技術を用いて、グローバルに社会の安全・安心を支えるソリューションを企画･事業化するためには、世界各地でまさに必要とされている技術を開発するとともに、ソリューション化までを迅速に行うことがますます重要になると考え、本技術を活用したソリューションの企画・開発を加速する「顔認証技術開発センター」を新設した。

本センターは、中央研究所で25年以上培ってきた顔認証技術をベースに、グローバルな課題にあった顔認証の新技術開発、およびソリューションの企画・開発を全社横断で推進するための組織だ。本センターは、社会インフラの高度化、新しい社会価値創造のためのソリューション提供などを担う「パブリックビジネスユニット」内に設置されている。NECは、本センターを通じて、世界各国のメンバーと連携し、本質的な社会課題の発掘・可視化、中央研究所による技術開発、ソリューションの企画・開発を推進していく。

NECは、セーフティ事業の中でも、特にグローバルに成長が見込まれる映像監視分野のソリューションへ新しい顔認証技術を適用することにより、さらなる事業拡大を目指していく考えだ。

● NEC　交通・都市基盤事業部
E-mail：inquiry@biometrics.jp.nec.com

オーシャンブリッジ

リモートコントロールツール「ISL Online」のワンタイム接続メジャーバージョンアップ版をリリース

オーシャンブリッジは、リモートコントロールツール「ISL Online」のワンタイム接続の最新版「ISL Light 4」の提供を開始した。今回の最新版は、オンプレミスライセンス、クラウドライセンスに対応し、次のような豊富な新機能が追加された。

・UIデザインの刷新：フラットデザインを採用してユーザビリティがより向上された。

・常駐接続も利用可能に：UI上からワンタイム接続、常駐接続の接続方式を「ワンクリックで」選択可能に。オペレーターはワンタイム、常駐接続をスムーズに行えることができるようになった。

・接続速度の改善：常駐接続を行う場合はクライアント端末への接続時間が10秒程度に大幅短縮。

・インストールの選択が可能：プログラムのインストールを行うことができるようになり、インストール後はWindowsの「プログラムの一覧」から高速起動が可能になった。

・セッションの停止･一時停止･再開：UI上で、セッションの停止・一時停止・再開ができるようになった。

・アクセスパスワードの保存：常駐接続にアクセスパスワードの保存機能が追加され、一度設定を行った端末に簡単に接続できるようになった。

・簡単ファイル転送：共有画面上にファイルをドラッグ＆ドロップして簡単にファイル転送が実行できる。

・システム情報の取得：接続先のシステム情報が簡単に取得できるようになった。

●オーシャンブリッジ
TEL：03-6809-0967

NEWS

アズジェント

公的機関向けに緊急時の情報資産流出を防ぐ「セキュリティ・プラス 自動遮断・設計／設定サービス」を提供開始

多くの公的機関にセキュリティ対策ツール導入の実績を持つアズジェントは、日本でいち早くリスクアセスメントを手がけた企業だ。公的機関でのリスクアセスメントの実績も豊富で、政府や行政業務、パブリック・セーフティに関連する方策を熟知した専門家により、業務への影響を最優先に配慮した自動遮断・設計を、リスクアセスメントを通して行っている。

同社のリスクアセスメントは、第三者的な評価で終わることなく、政府を含む公的機関固有のミッションに合わせて情報資産のリスク評価を行い、その上で、各 SIEM に精密な自動遮断のルールを設定する。これにより、業務継続への影響を最小限にしつつ、守るべき情報資産の流出に関連する端末やサーバ、通信経路のみを部分的に自動遮断することを可能にしている。

また、組織内で所有しているセキュリティ製品を最大限に活用した設計を行うと同時に、自動遮断を最適に実現するためのセキュリティ製品やネットワーク製品の選定や設計提案を、特定のベンダー製品に偏ることなく中立的に行っている。

このようなリスクアセスメントをもとに、各組織のスコープを明確化した「セキュリティ・プラス 自動遮断・設計 / 設定サービス」の提供を開始した。これは、公的機関が頻発するサイバー攻撃に備え、緊急時の情報資産の流出被害を防ぐことを目的としたサービスだ。

●アズジェント
TEL：03-6853-7402

セーファーインターネット協会

有害情報に「遺体・殺害行為に関する動画・画像」を追加
～遺族感情と表現の自由に配慮したガイドラインの改定を実施～

一般社団法人セーファーインターネット協会（以下、SIA）は、セーフライン運用ガイドラインを改定し、運用を開始することを発表した。主な改定内容は、ガイドラインの有害情報に「遺族の感情を著しく傷つける被害者の遺体や殺害行為の画像等」と「望まず閲覧してしまった人に著しく嫌悪感を抱かせる遺体や殺害行為の画像等」を追加するものだ。

過激派組織による拉致・殺害事件は国内に大きなショックを与えた。その際、遺体や殺害行為を撮影した動画や画像がインターネット上に流出したことで、「遺族感情を著しく傷つける」、「子どもや一般のインターネットユーザーに強いショックを与える」ものとして大きな社会問題となった。その反面、戦争やテロ等の悲惨さを訴える公共性の高い表現の中には、遺体や殺害行為に関する情報が含まれることがある。今回の改定では、表現の自由に最大限配慮しながら、遺族やこうした画像等の閲覧を希望しないインターネットユーザーを守るために、SIA が続けてきた議論の結果が反映されている。

なお、セーフラインでは、遺体や殺害行為にかかる動画や画像の全てに削除依頼を出すわけではない。表現の自由を最大限保護し、表現行為への萎縮を最小限に限定するため、問題となる画像や動画の内容、それらが掲載されている Web サイトの内容、削除を申告される方の立場等を個別の事案ごとに慎重に考慮して対応を進めていく。

●セーファーインターネット協会
TEL：03-6804-8539