



東芝が、運用リスク管理ソフトウェア「HUNTSMAN」を採用 ～不正アクセス・情報漏洩対策強化に～

株式会社MONET（本社：東京都千代田区、代表取締役社長：前野泰章）は、株式会社東芝の某主要工場にて、エンタープライズ向けセキュリティ/リスク管理ソリューション「**HUNTSMAN**（ハンツマン）」が採用されたことを本日発表致しました。

<HUNTSMANによる効率的なセキュリティ運用>

株式会社東芝の当該某工場では、企業の重要な資産である開発情報や製品情報を取り扱っております。既に様々なセキュリティツールが導入されておりますが、特に大規模な工場でのセキュリティを実現するためには、セキュリティ製品個別ではなく統合的に管理する必要があります。HUNTSMANを導入することで、個別のセキュリティ製品を統合的に管理すると共に、少ない人員で効率的に運用することが可能になりました。

<HUNTSMANによるセキュリティ強化>

企業ネットワークへのアクセスにはユーザID、パスワード等を利用するのが一般的です。しかし、ユーザID、パスワードの悪用により、なりすましによるアクセスも不可能ではありません。HUNTSMANは、ネットワークの定常状態を学習しプロファイルを作成することで、通常と異なるアクセスを発見することが可能になります。株式会社東芝の当該某工場では、なりすましによる不正アクセスを、HUNTSMANで自動監視し、セキュリティを更に強化しました。

<東芝某工場 採用ご担当者様のコメント>

弊社では、さまざまな情報セキュリティ強化施策を外部からの攻撃、内部からの漏洩対策として実施してまいりました。また、これらの施策によるログをみれば、危険な因子があるかどうかも理論的には掴めることとなります。しかしながら、このログが実は莫大な情報量です。1日に数万ラインにも及びとても何とかできる情報量ではありません。インシデントが発生した場合に、原因を追求する手段ができたにすぎないのが現状です。もしインシデントが発生したら、その対応・対策には膨大な労力をかけることになるのも現実です。

もし、ログ分析が簡単かつタイムリーに運用できれば、インシデントが発生する前に手を打つことで出来る可能性があり、結果発生そのものを抑えることができるかもしれない。「HUNTSMAN」は、この実現手段となりえます。それが理由で我々は採用しました。

<HUNTSMANの概要>

HUNTSMAN は、BAD（Behavioural Anomaly Detection: 異常挙動の自動検知）という、全く新しい発想に基づく脅威に対応する管理システムです。このBADは、ネットワーク上のハードウェア、ソフトウェア、OSなどから提供されるログに基づいたプロファイルを作成し、ネットワークの通常状態を学習します。このBAD技術によって、今までの技術では難しかった未知の（今現在、予測できない）脅威に対

する防御を可能にします。また、IT分野のリスクのみにとどまらず、企業のコンプライアンス管理に対するニーズも同時に満たすことができる画期的な技術です。

HUNTSMAN は、既にオーストラリアや英国の防衛、政府、重要インフラストラクチャ並びに金融業界など、高度なリスク管理が要求される分野で多くの実績があります。

内部統制の重要性が謳われている昨今、ログ収集の重要性と共に、運用リスクに対する管理は重要性を増しております。**HUNTSMAN**は管理者の負荷を軽減すると同時に、高度なセキュリティを提供いたします。

HUNTSMAN は運用リスクの管理と同時に、内部統制対策として利用されております。

「**HUNTSMAN**」の主な特徴

- ◆ 既知と未知の脅威に対する検知
 - BADテクノロジーによる異常挙動の自動検知
- ◆ 充実した分析機能
 - GUIベースでの多角的な分析機能
- ◆ リアルタイム機能
 - ダッシュボード（計器盤）機能によるモニタリング
 - シャットダウン
 - リモートでのコマンド実行
- ◆ レポート機能
 - インシデントの管理レポート
 - 運用・管理に関するレポート
 - スケジュール機能による定期的なレポート配信
- ◆ 管理者用の連絡機能
 - インシデント発生時の指示
 - 担当者の対応報告
 - 対応履歴
- ◆ フォレンジック
 - 証拠となるログ収集
- ◆ ユーザの操作履歴の監視

株式会社MONETについて

（株）MONETは、セキュリティおよびネットワークのソリューションプロバイダーとして2002年12月に設立した企業です。海外の優秀なベンダーとのパートナーシップを中心に、セキュリティ関連のソフトウェアの販売、コンサルティング事業を推進しています。他の主要取扱製品として、差分パッチ作成ソフトウェアであるPocket Soft社RTPatch / dfc-gorilla、情報漏洩対策ファイル暗号ソフトウェアのProtegrity社（旧OmniSecure社）のVPDisk Proがあります。

Tier-3社について

シドニーに本社を置くTier-3社は、**HUNTSMAN** における脅威管理システムの中心となる画期的なBAD（Behavioural Anomaly Detection：異常挙動の自動検知）テクノロジーを開発している企業です。**HUNTSMAN**では企業のセキュリティおよびリスク管理状況を監視することでより効果的なコンプライアンス管理が可能になります。また、**HUNTSMAN**によってはじめてアプリケーションやIP資産だけでなく企業のICTインフラストラクチャに及ぶ高度な管理が実現できます。Tier-3社は、防衛、政府、重要インフラストラクチャ並びに金融業界の各機関における幅広い顧客基盤を有し、その運営活動やコンプライアンス上の責任に対してより質の高いセキュリティおよびリスクの統合管理ソリューションを提供します。

お問合せ先

株式会社MONET

営業部

東京都千代田区三崎町3-6-15 東和水道橋ビル3F 〒101-0061

TEL : 03-3239-2430 FAX:03-3556-3248

Email : info@monetz.com

HP : www.monetz.com

*本文中の会社名および製品名は、各社の登録商標または、商標です。

Copyright 2007 MONET Co., Ltd. All rights reserved.