SF-SHERLOCK®

目 標

オートメーション化技術によりzプラットフォーム全体をカバーする最高のセキュリティ，最高のシステムクオリティを最小の労力で

包括的なリアルタイムモニタリングによる技術的プロテクションと法的規定への準拠

» RACF以来のメインフレームセキュリティ分野における最も重要なイノベーション «

zプラットフォームの完全なセキュリティモニタリング及びシステムモニタリング

インターネット，Eコマース全盛の時代，企業はリスクと危険を十分に認識し，大切な資産を守るために，より安全性の高いITセキュリティの実現に非常に高い価値を置いています。そうした中で，「メインフレームが最高のセキュリティによって守られている」ことが常に求められています。

Basel II（新BIS規格），IT Baseline Protection Manual（ドイツ連邦情報安全省ガイドライン），Sarbanes Oxley（米国SOX法），U.S.DOD Regulations, Gramm Leach Bliley Act(GLBA), KonTraG, RS FAIT 1, HIPPA Security, 95/46/EC Data Protection Directive 等の現行の法的規定や勧告，ISOやBS（英国規格）の認定基準等，あらゆる厳しい規格の下で，今日，企業には総合的なITベース業務プロセスの保護措置，その基底をなすテクノロジーを内部や外部からの攻撃に対して保護するための，きめ細やかで効率的かつ効果的な措置をとることが各国で求められています。日本でも，個人情報保護法の施行，ISMS認証，プライバシーマークの導入，来るべき日本版SOX法の施行等，企業のITをめぐるセキュリティ管理の徹底が急務になっています。市場における格付けで企業が良い評価を得るためには，技術面及び法律面でのスタンダード達成，セキュリティ面及びシステム運用面での最高のスタンダードの達成のために「可能な事は全てしている」という事を顧客，株主，所轄官庁，認定機関等に対して明示する必要があります。メインフレーム運用に際して，主要な課題となるのは，これらの要件を最小限の労力で達成することです。そのためには，ハイテクかつ効果的で，法的条件をクリアすることができ，すべてを自動で処理し，確実に仕事を処理することができる包括的なソリューションを探し出さなければなりません。

今日の市場競争を勝ち抜くための最も重要な要素は，セキュリティの完全化，品質管理の徹底，費用対効果の最適化です。日常業務のプロセスを見直し，品質向上と高度なオートメーション化によって生産性を大幅に高める事ができます。そして，それによって未来を切り開く「アクチュアル」で「アップ・トゥ・デート」なビジネスチャンスをものにする為に不可欠なもの―フレキシビリティと時間―を得る事ができるでしょう。

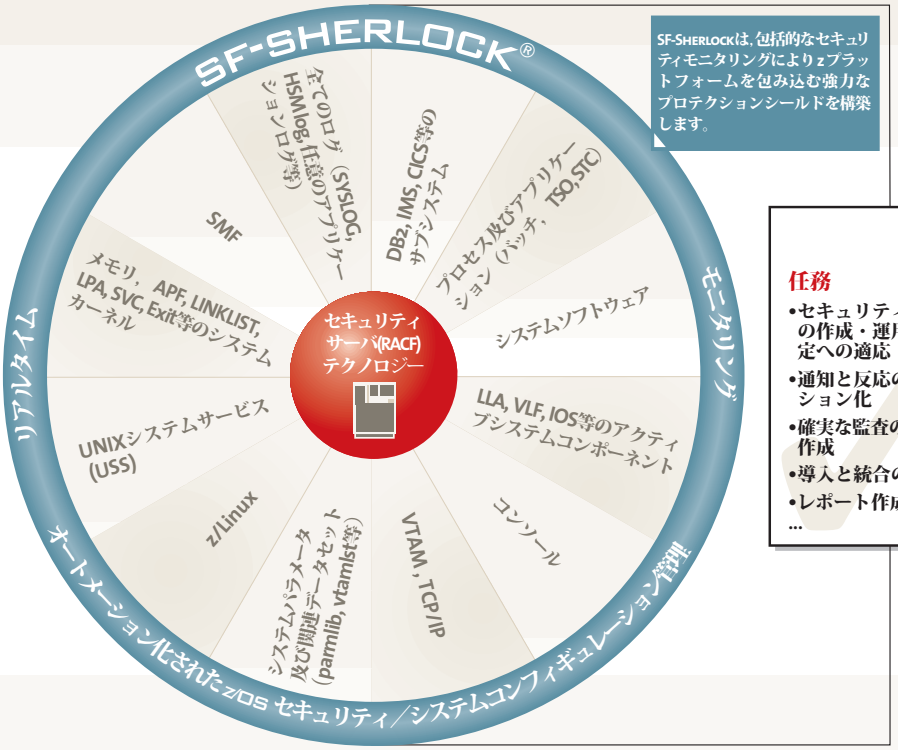
今日，求められているのは，イベントのリアルタイムでのモニタリング，コンスタントな脆弱性評価に基づくシステム内のウィークエリアの発見など，セキュリティ面で重要な処理をすべて実行するソリューション，メインフレームプラットフォームが正常に機能するために，技術的な意味でシステム領域すべてをカバーするソリューションです。同時に，日常の一般業務から，複数の部署・部門に渡る組織化された共同作業まで，あらゆる利用に耐えるソリューション，専門技術者からトップマネージャーまで，幅広い層のクライアントによる利用を想定したソリューションが求められています。

また，全社レベルでのクロスプラットフォームを一度に見渡し，一元的なセキュリティ管理・運営・監査ができるオープンなソリューション，更にITIL（英国商務局），CobiT（米国情報システムコントロール協会），BS7799，ISMS等の基準と調和し目的達成を確実にサポートする，投資に対する期待を裏切らないソリューションが必要とされています。

SF-SHERLOCKによるzプラットフォームのセキュリティ&システムクオリティオートメーションテクノロジーは，インターネットとEコマースの時代における新しいzアプリケーション分野に対する回答です。

パフォーマンス

- リアルタイムモニタリングによる24時間態勢のメインフレーム保護
- アプリケーションのモニタリング
- 省力化とコスト削減
- 総合的なシステム安定化
- アクセス権の濫用・盗用，並びに全てのプロトコル，ログ，メモリ改ざん等の探知
- 疑わしいイベントの探知及び論理トラップによる駆逐
- オートメーション化された通知と反応
- コンプライアンスチェック及びコンプライアンス監査
- イベント／ステータス管理に基づくファイルモニタリング
- 侵入者と漏洩者の監視
- 侵入と漏洩の探知
- SOX, KONTRAG, ISO, BS, U.S. DOD, BSI等の法的規定への準拠
- 全ての部署・部門への強力な支援
- 総合評価（スコアリング）付きセキュリティレポートの作成
- あらゆるマネージメントシステム，その他のITIL関連システムへの適合
- それぞれのクライアントに特化したレポート作成能力
- 悪用や不正変更に対する防御
- 分かりやすい統合インターフェース
- トラブルフリーの侵入テストによるコンスタントな脆弱性評価
- パスワード安全性テスト
- バッファオーバーフロー，書式制御ストリング等への攻撃に対する高いアプリケーション保護能力
- SMF，ログファイル等，あらゆる情報源のサポート
- 包括的なセキュリティチェックリスト
- 確実な監査結果の提示（ログ，セキュリティレポート等）
- IPL等のシミュレーション
- PARMLIB,VTAMLST等のシステムデータの構文チェック
- フルオートメーション化されたオペレーション
- クロスプラットフォームにおけるセキュリティ管理ソリューション，システム管理ソリューションの統合が容易なコネクションキット



任務

- セキュリティポリシーの作成・運用及び法規定への適応
- 通知と反応のオートメーション化
- 確実な監査のためのログ作成
- 導入と統合の簡素化
- レポート作成

...

私たちが提案するソリューション：
SF-SHERLOCK リアルタイムセキュリティ＆システムモニタリング

»**テクノロジー**: SF-Sherlockは，モニタリング，レコード書き込み，通知，反応，レポート，IPL等のシミュレーションの可能性を統合する事によって，zプラットフォーム上で完全なセキュリティとシステムコンフィギュレーションのオートメーション化を確立するための高性能リアルタイムモニタリングソリューションです。これは，システム上で常に稼働しているプロセス，すなわちセキュリティシステム（セキュリティサーバ，あるいはCA-TopSecret, CA-ACF2等のRACF)や特殊なプロセス，あるいはサブシステム（DB2, LDAP等）やz/OSを，そのコンポーネントと共にモニタリングし検証します。重要な変更における監査情報を正確に記録し，管轄部門の管理者に対して個別に，エラー，攻撃，改ざん，変更等，その領域に関連したイベントを，Eメールや SMS（携帯電話ショートメールサービス）で，ジャスト・イン・タイムで通知します。それに応じて，監査部門に自動的にリアルタイムのモニタリング結果，セキュリティレポートと総合評価を送ります。これは，全行程が自動化されている事を意味しています。そのために誰かがその都度，煩雑なルーチン作業をする必要はもうありません。このオートメーション化技術がフレキシビリティとセキュリティを同時に実現します。SF-Sherlockのオートメーション化技術は，決定的な事態に対してレポートするだけではありません。例えば，不法な侵入者を瞬時にシステム外に追放する事も自動的に行います。絶え間ない制御と監視により，文字通り「24時間体制のメインフレーム保護」が実現し，システム全体にわたるトップレベルのセキュリティとコスト削減の両方を一度に手にする事ができるわけです。

»**絶える事のない需要**: 2004年以来，ドイツ連邦情報安全省(BSI)は，メインフレームプラットフォーム運用に欠かす事のできない基準を，そのセキュリティ・ガイドライン「IT分野における保護に関する基本指針」で規定しています。その中では，「セキュリティ侵害をより迅速に検知するためにz/OSシステムにはリアルタイムで動作するセキュリティモニタを導入すべきである」との要旨が述べられています。SMFによるレコード書き込みのように，単独のセキュリティシステムによるリアルタイムモニタリングでは，十分なセキュリティが確保できているとは言えません。セキュリティ確保に欠かせないのは，z/OSの全てのコンポーネント，並びにその細部にまでわたる複雑な相互関係までをモニタリングする事です。SF-Sherlockは，z/OSの内部に潜在している「トリッキーな」危険性や隠されたエラーから，より高い権限を必要とするレベルでのオーディットトレイルの破壊，データバンクをはじめとする様々なリソースに対する秘密裏の不正アクセスまで，z/OSシステムを包括的かつ完全にモニタリングします。不正アクセスのプロたちは，目標とするデータにアクセスし，スパイ行為をはたらき，セキュリティシステムを操作して，SMFやログファイルにその形跡を残しません。それに起因して，気づかれずに残っているシステムパラメータやコンフィギュレーションのエラーは，システム全体の運用可能性やIPLに影響を与え，遅くとも次回の起動時に問題をもたらすかもしれません。これらのセキュリティの欠陥やシステムの障害は，ビジネスに大きな損害をもたらすため，絶対に防がなければなりません。だからこそSF-Sherlockは，セキュリティシステムのチェックに加え，パラメータライブラリやその他の重要なシステムファイルを自動的にチェックし，予期される欠陥やエラーを発見します。また，ハッカーによる不正操作は非常に短時間で完結します。そうした中で，常に監視の目を光らせているのが，リアルタイムテクノロジーです。機敏な反応による不正行為の探知と防止，徹底した形跡の提示――これらはリアルタイムテクノロジー抜きにしては実現できません。潜在する脆弱性やエラーに関して，チェックされるべき項目は非常に多岐に渡り，また広範囲に及んでいます。これをクリアする事ができるのは完全にオートメーション化されたモニタリングの実現をおいて他にはありません。

»**成功を保証するテクノロジー**: オートメーション化され，包括的かつ確実に作動するSF-Sherlockのテクノロジーは，最高の目標設定とその実現をを完全にサポートし，メインフレームプラットフォームを様々な要求に応じて適切に制御し，健全に稼働させます。SF-Sherlockをもってすれば，必要不可欠な要求に応える事だけでなく，システム全体の安定性と包括的な情報リソースの保護の両方を一度に手に入れる事が可能です。SF-Sherlockの導入によって，ビジネスの将来は，より確実なものとなるでしょう。絶え間ない完全なモニタリングと検査は，殊に非常に高度な技術レベルでの利用において，z/OSの新機能（UNIXシステムサービス，Sysplexテクノロジー等）やWebサーバ，データサーバ，Eコマースプラットフォーム等の新しいアプリケーション群とともにその真価を発揮するでしょう。現行のセキュリティスタンダードは，徐々に不十分なものとして感じられるようになるはずです。内部，外部からの不正侵入／情報漏洩に対する検知・防御システムとしてのSF-Sherlockの機能は，今まで閉ざされていたシステムのオープン化と外部へのネットワーキングの流れの中で，最高レベルのITリソース保護を提供するものとして，その意味はますます大きくなるでしょう。この先進的なテクノロジーにより，SF-Sherlockは，今後も，常にリスクと戦っている最先端のセキュリティ水準を押し上げ，同時にシステムの健全な運用を保証するという，先進的且つ必要不可欠な歩みを進めて行きます。

»**成功を保証する生産性**: SF-Sherlockは，セキュリティアドミニストレーション部門，セキュリティ監査部門，データ・情報管理部門，システムアドミニストレーション部門で，自動制御のリアルタイムプロセスとして動作します。さらに，各部門において共通性の高い効率的なワークフローを構築することにより，高生産性，大幅なコスト削減を実現します。SF-Sherlockは，包括的なセキュリティとオートメーション化により，企業内のクロスプラットフォーム環境を統合するソリューションとして，最高の収益性と経済性をもたらします。プラグアンドプレイな実装コンセプトにより，これらの目的を，複雑な手順を踏むことなく達成し，それに必要な業務 ―― 例えば，法規制への適応，セキュリティポリシーの作成・運用など―― に費やす時間やコスト，労力を軽減します。

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM