FIREEYE™

ネットワーク・フォレンジック

高速なパケット・キャプチャおよび調査解析機能により ネットワーク攻撃の影響を最小化

サイバー攻撃の影響を最小限に抑えるためには、インシデントの早期発見と速やかな調査が必要です。調査結果に基づいて影響の範囲と深刻度を特定し、セキュリティ脅威を確実に封じ込めて、再発防止策を講じる必要があります。

FireEye Network Forensicsは、一元的な解析および視覚表示を可能にしながら、業界最速で、ロスのないネットワーク・データのキャプチャとデータの検索が可能なソリューションです。調査を効率化し、リスクを低減する単一のワークベンチを使用するため、ネットワーク・フォレンジック調査を高速に実施できます。

FireEye Network Forensicsは、フル・パケットを超高速でキャプチャしてインデックス化し、セキュリティ・インシデントを迅速に確認、解決することができます。幅広いセキュリティ・インシデントの検知、インシデント対応の強化、それぞれのインシデントがもたらす影響の正確な定量化を可能にします。

FireEye Network Forensicsソリューションの一部である調査解析システムは、使いやすい解析インタフェースを備える一元的なワークベンチにより、ネットワークに潜むセキュリティ脅威の早期発見と迅速なインシデント対応を実現します。

アナリストは、攻撃の前後および攻撃中にやり取りされている特定のネットワーク・パケットやセッションを詳しく把握できます。マルウェアのダウンロードやコールバックを引き起こしているイベントを再現し、視覚的な確認を行えることで、素早く効果的なインシデントレスポンスや再発防止を可能にします。ネットワーク内の攻撃の展開に一般的に使用されるプロトコルをデコードするので、攻撃者の活動に対する可視性も高まります。

詳細な解析機能とパフォーマンスに優れたパケット・キャプチャ機能を独自に組み合わせることで、攻撃のあらゆる構成要素をすばやく認識して監視できます。

図1: パケット・キャプチャおよび解析機能用のFireEye Network Forensicsアプライアンス

パケット・キャプチャのハイライト

- **高性能：**継続的でロスのないパケット・キャプチャを、最大20 Gbpsの速度で、タイム・スタンプ付きで実現
- **高精度：**タイム・スタンプと接続属性を使用して、キャプチャしたすべてのパケットをリアルタイムでインデックス化。フロー・インデックスと接続メタデータをJSON形式でエクスポート。フロー・インデックスは、NetFlow v9、IPFIX、Silk Toolsのデータ形式に変換可能
- **すばやい結果表示：**特許取得済みのインデックス化アーキテクチャを使用して、目的のコネクションやパケットを超高速検索
- **豊富なコンテキスト：**Webベースのドリルダウン型GUIを使用して、パケット、接続、セッションを検索、解析
- **包括的な可視化：**セッション・デコーダーでパケット解析を実施し、Web、Eメール、FTP、DNS、チャット、SSL接続の詳細や添付ファイルを可視化、検索
- **インテリジェントなキャプチャ：**キャプチャしたトラフィックをフィルタリングし、ストリーミング・ビデオ、大きなファイルの転送、暗号化されたペイロードなどを排除
- **効率を向上：**データ窃取の検知プロセスを自動化。独自のアルゴリズムを使用して、ネットワーク上の潜在的に異常な振る舞いを検証

表1：使用可能なパケット・キャプチャ・アプライアンス

モデル	キャプチャ・ポートの構成	管理ポート	記録速度（最高）	オンボードのストレージ容量（合計）	寸法	電源/標準的な動作負荷
PX 1004S-6	4 x 1GbE	2 x 1GbE	500 Mbps	6 TB	1U 437×500×44 mm 8.2 kg	AC、100～240 VAC（固定）（50～60 Hz時）、IEC60320-C14インレット
PX 2060ESS-96	4 x 10GE SFP+	2 x 1GbE	2 Gbps	96 TB、拡張SAS接続ストレージ	2U 438×620×88.4 mm 26.0 kg	冗長電源（1+1）800W、100～240 VAC、10.5～4.0 A、50～60 Hz、IEC60320-C14インレット、フィールド交換対応
PX 2060ESS-120	4 x 10GE SFP+	2 x 1GbE	7.5 Gbps	120 TB、拡張SAS接続ストレージ	2U 438×620×88.4 mm 26.0 kg	冗長電源（1+1）800W、100～240 VAC、10.5～4.0 A、50～60 Hz、IEC60320-C14インレット、フィールド交換対応
PX 1004EXT-4G	1 Gbps、10/100/1000 BaseT、SFP 4ポート	10/100/1000 BASE-T 2ポート、10/100/1000/10G BASE-T 2ポート	4 Gbps	オンボード・ストレージなし。ファイバチャネルHBAで外部FC-SANストレージに接続	1Uラックマウント、 4.3×43.7×65.0 cm 20.9 kg	650W高効率（1+1）冗長AC電源、100～240 VAC、60-50 Hz（自動切替え）、230～280W（標準的な環境の場合）
PX 1040EXT-20G	1 Gbps 4ポート	10/100/1000 BASE-T 2ポート、10/100/1000/10G BASE-T 2ポート	20 Gbps	オンボード・ストレージなし。ファイバチャネルHBAで外部FC-SANストレージに接続	1Uラックマウント、 4.3×43.7×65.0 cm 20.9 kg	650W高効率（1+1）冗長AC電源、100～240 VAC、60-50 Hz（自動切替え）、230～280W（標準的な環境の場合）
PX 4000SX440	N/A	N/A	N/A	440TB、RAWストレージシェルフ	437×698×178 mm 34 kg	1280W高効率（1+1）冗長AC電源、100～240 VAC、60-50 Hz（自動切替え）

注：パフォーマンス値は、システム構成や処理するトラフィックの特性によって異なります。

FireEye調査解析システムは、単一ノードまたは分散アーキテクチャ向けにさまざまな構成をサポートしており、ネットワーク帯域幅の消費やメタデータの集約、照会、解析のパフォーマンスを最適化できます。

調査解析のハイライト

- **視覚化：**容易にカスタマイズ可能なダッシュボードで、ネットワークのメタデータとイベントを視覚化し共有
- **高速照会：**すべてのアラート、キャプチャしたフロー、およびメタデータに対し、アプリケーションレベルのキーワード、正規表現、およびワイルドカードを使用した照会を一元的に実施
- **即応性に優れたインタフェース：**対象セッションのPCAP形式の各データまたは一括データを即座にアクセスしてダウンロード
- **強力な検索：**HTTP、SMTP、POP3、IMAP、SSL、TLS、DNS、FTPなど多様なプロトコルにわたるメタデータをインデックス化し、迅速に検索
- **IOCの集約：**単一のワークベンチでFireEyeネットワーク・セキュリティ、Eメール・セキュリティ、エンドポイント・セキュリティの製品からのアラートをすべてのネットワーク・メタデータとともに集約し、アラートからセッション・データに「ワンクリック」ですぐにアクセス
- **セキュリティ脅威のレトロスペクティブな探索：**iSIGHT、STIX、OpenIOCフィードを自動IA検索機能と統合することにより、「過去にさかのぼって」IOCのセキュリティ脅威を解析。ネットワークに存在するIOCに対するアラートを数日前から数週間前に自動的に配信
- **ワンクリックでファイルを再構築：**疑わしいファイル、Webページ、Eメールを素早く安全に再構築して、さらなる解析を実施

表2：使用可能な調査解析アプライアンス

モデル	オンボードのストレージ容量（合計）	寸法	電源/標準的な動作負荷
IA 1000 DIR	6 TB	437×500×44 mm	AC、100～240 VAC（固定）（50～60 Hz時）、IEC60320-C14インレット
IA 2100-48	48 TB	437×500×44 mm	冗長電源（1+1）800W、100～240 VAC、10.5-4.0 A、50～60 Hz、IEC60320-C14インレット、フィールド交換対応

FireEyeの詳細については、**www.FireEye.jp**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03－4577－4401 |
Japan@fireeye.com

会社概要
FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデント対応といった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。