平成 23 年度
政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書

平成 24 年 3 月

内閣官房情報セキュリティセンター

改版履歴

版	日付	改版内容
1.0 版	平成 24 年 3 月	初版
1.1 版	平成 24 年 10 月 1 日	誤記の修正

目次

1. 検討の背景 4
1.1 背景・課題認識 4
1.2 検討内容 4
2. 検討結果 5
2.1 総括 5
2.2 すぐに実施可能な推奨対策 5
2.3 今後の課題、方向性 7
3. 検討会概要 8
3.1 検討会の開催 8
3.2 検討会構成員 8
3.3 検討会の概要 9
3.3.1 第 1 回検討会（2011.11.15）の概要 9
3.3.2 第 2 回検討会（2011.11.18）の概要 9
3.3.3 第 3 回検討会（2011.12.9）の概要 10
3.3.4 第 4 回検討会（2011.12.20）の概要 10
3.3.5 第 5 回検討会（2012.1.17）の概要 11
3.3.6 第 6 回検討会（2012.2.28）の概要 11
3.3.7 第 7 回検討会（2012.3.29）の概要 12
4. 情報収集業務の概要 13
4.1 情報収集業務の調査項目 13
4.2 （ア）民間企業からの不正アクセス等のヒアリング結果 14
4.2.1 ヒアリング対象の選定 14
4.2.2 ヒアリング項目及び方法 14
4.2.3 ヒアリング結果概要 14
4.2.4 ヒアリング結果詳細 15
4.2.5 その他ヒアリング全体に関する所感（作業委託発注会社によるもの） 17
4.3 （イ）ログ・証跡管理に関する製品およびサービス調査結果 18
4.3.1 調査方法 18
4.3.2 調査対象製品・サービス 18
4.3.3 調査項目 18
4.3.4 調査結果 19
4.3.5 備考：ログ・証跡管理製品・サービスを比較するポイント 20
4.4 （ウ）ログ・証跡管理に関する報告書調査結果 22
4.4.1 調査方法 22

4.4.2　結果 22
4.5　（エ）海外政府機関及びそれに準ずるログ・証跡管理に関わる報告書やガイドラインの調査結果 .22
4.5.1　調査方法 22
4.5.2　結果 22

1. 検討の背景

1.1　背景・課題認識

これまで政府機関においては、情報システムにおけるログの収集・管理等に係る統一的な基準が定められておらず、各省はシステムの用途や監査等の個別の事情に応じてこれを行ってきた。また、ログのなかでも高い証拠性が求められる証跡については、「政府機関の情報セキュリティ対策のための統一基準群」（平成 23 年 4 月 21 日情報セキュリティ政策会議決定）において証跡管理機能の導入に係る対策基準を定めているが、具体的な対策内容については、各府省庁の判断に委ねられている。

一方、標的型攻撃等の新しいタイプの攻撃が増加している状況において、情報システムにおける適切なログ収集・管理を行うことで、この種の攻撃の検知や攻撃成功後の事実確認等に資することが出来る可能性が考えられる。しかし、上述したログの収集・管理等に係る統一的な基準が定められていないこともあり、各省におけるログ取得・管理の取組は、必ずしも十分とは言えない。

その他、新しいタイプの攻撃への対応だけでなく、ログの収集・管理に関する課題は、電子政府の推進や裁判実務における利用等、広範な分野において存在している。

1.2　検討内容

情報セキュリティやフォレンジック技術等の専門家を構成員とする検討会（事務局：内閣官房情報セキュリティセンター）により、標的型攻撃等の新しいタイプの攻撃への対応という観点を中心に下記検討を行った。

- 政府機関における情報システムのログの取得・管理の在り方に関する課題整理、課題の優先度付け
- 新たな脅威や攻撃手法の類型毎の、対策にあたり望ましいログの取得・管理の内容（対象、保存期間、解析手法等）
- 統一基準上の遵守事項として実施するべきログの取得・管理の内容　等

検討では、専門家の知見を踏まえ、現状の課題認識やその優先順位を整理するとともに、適切なログ収集・管理の統一的な基準を導出していくことに資する検討会および調査を実施した。

2. 検討結果

2.1 総括

標的型攻撃等の新しいタイプの攻撃の検知や攻撃成功後の事実確認等への活用という観点を中心に、ログを取得する機器や構成、ログを取得する対象（種類やパラメータ）、ログ解析手法、ログ保存期間、ログ取得・管理に必要な費用等について、専門家の意見を反映しながら調査・整理を行った。その結果、新しいタイプの攻撃に対してある種のログ取得・管理が有効であることを明らかにした。一方、これを実施するための費用が高いものがある、有用性について意識や知見が十分に浸透していない、といった課題があることも明らかとなった。

これらの結果を踏まえ、現在増加している標的型攻撃に対する一つの対処策として、比較的すぐに実施可能なログ取得・管理の推奨対策を取りまとめた。本内容については、各省庁に情報提供をするなどして、適切なログ取得・管理の取組を支援していくことが重要である。また、本内容を適切な形で「政府機関の情報セキュリティ対策のための統一基準群」に盛り込むことで、各省の情報セキュリティ対策に関するPDCAサイクルに適切に組み込まれるがことが望ましい。

2.2 すぐに実施可能な推奨対策

検討会の議論を踏まえ、政府機関において「すぐに実施可能な推奨対策」を取りまとめた。なお、括弧内＜＞は、「政府機関の情報セキュリティのための統一基準群」（2012 年 4 月 26 日 情報セキュリティ政策会議決定）上の関連する遵守事項を指す。

I. 機器によらない全般的な対策

1. 各ログ取得機器のシステム時刻を、タイムサーバを用いて同期する。

＜2.3.2.2(2)(d), 2.3.2.3.(2)(d),2.3.4.1(2)(e)＞

- ○ 調査時の複数機器のログの解析を迅速かつ十分に実施するため。（各ログの時刻が数秒ずれていても、これを補正する作業は大変困難である。）
- ○ 各ログ取得機器は、タイムサーバを用いた時刻同期ログについても取得する。
- ○ 精度や冗長性を高めるため、各ログ取得機器組織内ネットワークに設置したタイムサーバ（stratum2 サーバ）と代替のタイムサーバの複数のタイムサーバを利用することが望ましい。

2. ログは1年間以上保存する。

- ○ 過去の標的型攻撃事例から、攻撃事象の発見からさかのぼると攻撃の実施された時期はおおよそ 1 年以内であり、ログを1年間保存すれば、高い確率で攻撃の初期段階からのログを抽出することができるため。

3. 複数のログ取得機器のログを、ログサーバを用いて一括取得する。

- ○ 攻撃者によるログの改ざんを簡便に防ぐことが出来るため。

○ ログサーバのアクセス権を最小限とすることが望ましい。また、ログサーバについては、改ざん防止のために内部ネットワークに置く必要がある。

○ 高スペックな機器を利用する必要は無い。

4. 攻撃等の事象発生が確認された場合の対処手順を整備する。

＜1.2.2.2(1)(c)＞

○ 攻撃等の事象発生が確認された場合に取るべき行動を検討し周知すること。不必要な行動をとってしまうことでログが上書きされ、原因究明が困難になってしまう恐れがあるため。

II. 機器別の対策

1. ファイアウォール:「外⇒内で許可した通信」と「内⇒外で許可・不許可両方の通信」のログを取得する。

○ 外部の攻撃者により侵入された通信と、その後のバックドア通信を把握するため。

○ 攻撃への対策とログ解析の効率化のため、外→内の通信は必要なものに限定することが望ましい。

2. Web プロキシサーバ:接続を要求した端末を識別できるログを取得する。

○ バックドア通信で多く用いられる HTTP/HTTPS の情報から、C&C サーバの IP アドレス・感染端末の特定・活動の実態を把握するため。

3. 他のシステムや機器の権限を管理するサーバ(LDAP, Radius 等):管理者権限による操作ログを取得する。

○ 管理者権限の窃取等を把握するため。

4. メールサーバ:「メールの送受信アドレス」及び「メッセージ ID」のログを取得する。また、出来る限り「添付ファイル名」のログを取得する。

○ 標的型メールのログから、攻撃者が利用するサーバや、攻撃に利用したマルウェアの情報を把握するため。

○ 情報の窃盗(アップロード)に SMTP を利用するケースが見られるため。

○ マルウェア対策ソフトウェアで検知できないマルウェアの情報を把握するため。

5. クライアント PC:マルウェア対策ソフトウェアの検知・スキャンログ・パターンファイルのアップデートログを取得する。

○ マルウェアによる感染の実態を把握するため。

6. DB サーバ・ファイルサーバ:特別なログ設定は不要だが、確実にログを取得する。

○ 窃盗された情報等、攻撃を把握するために重要であるため。

2.3 今後の課題、方向性

検討会で議論された、政府機関における情報システムのログ収集・管理に係る今後の課題を下記に列挙する。

○ 統一基準の改定／マニュアルの策定
- 情報システムのログ取得・管理に関し、政府機関が最低限遵守すべき事項について検討し、必要な事項については政府機関の情報セキュリティ対策のための統一基準群を改定しこれを盛り込む。
- 情報システムのログ取得・管理に関し、政府機関がその実施に際して有用となる具体的な情報を取りまとめ、マニュアルとして策定する。

○ ログの在り方についてのさらなる検討・整理
- 「標的型攻撃等の新しいタイプの攻撃対策」以外の目的も含めた一般論としてのログの在り方について検討する。具体的には、「標的型攻撃等の新しいタイプの攻撃以外のセキュリティインシデント」「システム利用状況」「システム障害」「個人情報の漏えい・改ざん・紛失」「業務ルール違反」「監査」「データ保存及び更新時の記録取得」等を考慮することが挙げられる。
- ログの管理レベルに応じた仕組みを検討する。例えば、「単純にログを取得し特別な仕組みは設けない」「第三者による不正が出来ない仕組み」「管理者であっても不正が出来ない仕組み（最小権限・権限分散等）」等が考えられる。
- 「ログ」と「証跡」の違いについて整理する。例えば、ログと証跡の違いを明らかにし、これを定義する（デジタル・フォレンジック研究会（IDF）との連携）。また、政府機関内で証跡が必要となるケースや条件の抽出や具体的な証跡管理手法を検討する。法律的観点での真正性（推定効）の考慮について検討する、などが挙げられる。

○ その他
- ログ取得・保存にかかる費用の精査・事前見積り方法を検討する。
- クラウド等アウトソーシングサービス利用時のログ・証跡の扱いについて整理する。例えば、政府機関が契約時に SLA(Service Level Agreement)で確認すべき内容の検討、などが挙げられる。

3. 検討会概要

3.1 検討会の開催

「1. 検討の背景」において示された課題を検討するため、内閣官房情報セキュリティセンターにおいて、「政府機関における証跡管理の在り方に関する検討会」を開催し、議論を行った。

○ 検討内容
- 政府機関における証跡管理の在り方に関する課題整理、課題の優先度付け
- 政府機関における適切なログ管理の在り方
- (特にフォレンジック等の観点から)ログを使用する専門家から見た、新しい攻撃に係る検知、事後の対処に必要なログの種類、期間等の具体的な内容
- 民間事例の紹介

○ 検討会の最終成果イメージ

各種攻撃対策としての情報システムのログ取得の在り方に関し…
- 各府省庁に事務連絡を発出 (本年度末を目途)
- 「すぐに実施可能で、ある程度の効果が望める対処」を記載
- ログ取得に係る推奨マニュアルの策定 (来年度下期を目途)
- 「高い効果が望める理想的な対処およびその具体例」を記載
- 中長期的に実施するような、全体システム設計時の推奨事項
- 代表的な製品における設定例を含む詳細な情報 等について記載
- 統一基準群の改定 (平成 24 年度改定版)
- 各府省庁に求める最低限の対処事項を追加

3.2 検討会構成員

本検討会は、以下の構成員等により開催した。(敬称略)

構成員	
東京電機大学 未来科学部教授(NISC 情報セキュリティ補佐官)	佐々木良一(座長)
株式会社UBIC 執行役員	野崎 周作
総務省情報通信国際戦略局通信規格課 標準化推進官	上原哲太郎
ネットエージェント株式会社 フォレンジックエバンジェリスト	松本 隆
株式会社サイバーディフェンス研究所 情報分析部 上級分析官	山田 晃
株式会社サイバーディフェンス研究所 情報分析部 部長	名和 利男
Payment Card Forensics 株式会社 取締役	瀬田 陽介
特定非営利活動法人デジタル・フォレンジック研究会 理事・事務局長	丸谷 俊博
株式会社KPMGFAS ディレクター	上原 豊史

株式会社UBIC　取締役	長谷部泰幸
委託調査会社	
株式会社ディアイティ　セキュリティサービス事業部　事業部長	青嶋　信仁
株式会社ディアイティ　セキュリティサービス事業部　部長	山田　英史
事務局:内閣官房情報セキュリティセンター	
内閣参事官(政府機関総合対策促進担当)	木本　裕司
情報セキュリティ指導専門官	佐藤　慶浩
情報セキュリティ指導専門官	丸山　満彦
情報セキュリティ指導専門官	冨士原裕文
情報セキュリティ指導専門官	榎木　千昭
政府機関総合対策促進グループ	

3.3　検討会の概要

本検討会は、平成 23 年 11 月～平成 24 年 3 月の期間において、計 7 回開催した。各回における議論の概要を以下に記載する。

3.3.1　第 1 回検討会（2011.11.15）の概要

○　「新しい攻撃法とフォレンジックに関する考察」（東京電機大学教授　佐々木良一氏）
- 検討会の趣旨と方向性の案について議論。

○　「新しい攻撃とフォレンジックについて」（ネットエージェント株式会社　松本　隆氏）
- クライアントPC(Windows)におけるログ取得(Volume Shadow Copy Serviceによるボリュームのバックアップや、CrashDump による完全メモリダンプ等)により、過去に存在していたマルウェアの検出が可能となる場合がある。
- パケットキャプチャは、各種不正イベントの検出に有効。
- 相関解析を行う上では、各ログ取得機器の時刻同期が重要。

○　ディスカッション
- 検討会の今後の方向性として、まずは「すぐ実施できること」をリストアップするべき。
  （具体例:ログ取得を行うべきもの、FW の Outbound、IDS の Outgoing、プロキシ接続先　等）
- 推奨するログ保存期間も、具体的に定めるべき。
- ログは各サーバで管理するのではなく、ログサーバで一元管理すべき。

3.3.2　第 2 回検討会（2011.11.18）の概要

○　「新しい攻撃法とフォレンジックに関する考察」（東京電機大学教授　佐々木良一氏）
- 勉強会の趣旨と方向性の案について議論。

○　「標的型攻撃に対する防御」（Payment Card Forensics 株式会社　瀬田陽介氏）
- PCI DSS の要件のうち、標的型攻撃に関連するものをピックアップして紹介。

- 重要な情報へのアクセスや操作のイベントを再現するために、すべてのシステムコンポーネントの自動監査証跡を実装する。
- 時刻同期、監査証跡の保護、ログの監視について規定。
- ログ取得対象：ルータ／ファイアウォール、VPN アクセス、OS(Windows/Mac)、ウイルススキャン、IDS/IPS、Web/AP/DB、ファイルサーバアクセス、認証ログ（ActiveDirectory/LDAP/Radius）、メインフレーム、ワイヤレスアクセス、クライアントログ、タイムサーバ（NPT など）
- ログ取得内容：ユーザ識別、イベントの種類、日付と時刻、成功又は失敗を示す情報、イベントの発生元、影響を受けるデータ・システムコンポーネントまたはリソースの ID または名前。
- 統合ログ管理ツールによるログ取得、監査ログ自体の監査性の保証
- 監査証跡は、直近 3 ヶ月は手元に置いておき、1 年間は保管する。（1 年間では短いとの意見もあり）

○ ディスカッション

- 統合ログ管理ツール RSA enVison は有効だが、IT 統制機能が含まれておりオーバースペックで高価である。
- 実際の相関解析は、ツールを利用するのではなく手作業で行っている。

3.3.3 第 3 回検討会（2011.12.9）の概要

○ 「新しい攻撃法と証跡管理に関する考察」（株式会社 UBIC 長谷部泰幸氏）

- FW のログから分かる情報：社内セキュリティポリシー違反、不審なファイアウォールアクセス、DMZ からの不審な通信、社外からの社内アクセス（VPN）、狙われているサービス、攻撃者 IP、ネットワークプロービング(ICMP)、コントロールされていない通信、長時間セッション、大量通信、ループバックアドレスからの通信、危険なサービス、高頻度使用ルール、未使用ルール

○ 「不正調査時のログに関する問題点、調査時で有効であったログ」（株式会社KPMGFAS 上原豊史氏）

- 重要情報を定義し、それが格納されているデータベースへのアクセスログをもれなく収集すべき。
- 重要なログは消去や改ざん防止を行った上で収集し、1 年（できれば 2 年）保管すべき。
- ログの取得だけ熱心になるのではなく、その解析もあわせて重要。
- 実際に有効であったログ：データベースのアクセスログ、PC の操作ログ、外部デバイスの接続ログ、電子メールのアーカイブ、入退出ログ

○ ディスカッション

- マルウェアが行う通信を把握する方法について優先度をつけて整理すべき。
- 内部→外部の DNS のキャッシュやクエリのログは、攻撃の偵察段階の把握に有効。
- フォレンジックとしては、クエリのログと syslog の両方セットでないと意味がない。
- ゲートウェイ上にあるものは網羅的にログを取得することを緊急対策とするのがよい。
- ルータや L3 スイッチによる内部→内部通信のログが、攻撃の検知に有用。

3.3.4 第 4 回検討会（2011.12.20）の概要

○ 「調査を前提としたログの取得」（ネットエージェント株式会社 松本隆氏）

- 監視（≒動的解析）とデジタルフォレンジック（≒静的解析）とはログの用いられ方が違う

- デジタルフォレンジック調査の最優先事項は、取得しているログを把握すること。
- 目的（検知 or 事実確認、何を明らかにするか、等）によってどのログを取得するかが異なる。

○ 「ISO/IEC 270XX シリーズ標準化の動向」（サイバーディフェンス研究所　山田晃氏）
- 標準化（IS 発行）までの工程は平均 2.8 年。
- 27037（証拠的価値があると考えられる「潜在的デジタル証拠」の特定、収集、取得及び保全に関する指針）：DIS 行程のため、1 年以内に発行予定。
- 27042（Guidelines for the analysis and interpretation of digital evidence）：NP 工程開始。

○ ディスカッション
- IDS やファイルサーバのアクセスログについての検討が必要。
- 「監視の観点」と「保全の観点」で整理するとよい。
- ログ取得・解析をする前提として、システム構成が適切であることが必須。例えば、外部との通信経路は FW 経由のみとし、各種機器の不要なポートを閉じるなど。さもないと、そもそも守りたい攻撃対策になっていないばかりか、攻撃の情報がログに残らないといった事態となる。
- Proxy を認証 proxy とすると、ユーザが判別できるのでログの観点からは良い。ただし費用が高い。
- タイムサーバへの同期ログ、コマンドログ、ログのリセットログの取得が重要。

3.3.5　第 5 回検討会（2012.1.17）の概要

○ ディスカッション
- 以下の資料等を参考に、ログに関する対策を取りまとめてはどうか。
- NIST SP800-92「Guide to Computer Security Log Management」
- データベース・セキュリティ・コンソーシアム「統合ログ管理サービスガイドライン（ver1.0）」
- FIRST「Critical Job Review」
- 取得、保管、解析、監視のフェーズに分けて議論を行うべき。
- （取得、保管：各省庁で対応。解析、監視：主に外部委託で対応）
- 衆議院、参議院の事例も参考に、取得すべきログ等を検討。

○ 「すぐに実施可能な推奨対策」について
- 基本的な考え方や対策については、NIST 等の文献を参照してもらう
- 記載内容は既存の文献で想定をしていない標的型攻撃を前提とし、対策として低コストで特に有効と思われる項目について、既存の文献に無い具体的な推奨パラメータ　とする
- フォレンジック的なものに限定し、動的なものは記載しない（ガイドライン側で対応する）。

3.3.6　第 6 回検討会（2012.2.28）の概要

○ 外部委託調査　中間報告（株式会社ディアイティ　青嶋　信仁氏）
- 重要インフラ企業数社へのヒアリング：運用の外部委託でログも含め状況を把握していないケース多。
- 製品及びサービス調査：ログ保存、収集、管理する機能中心で調査中。
- 報告書：調査中だが見つかっていない
- 海外事例：10例ほどピックアップしている。

○ ディスカッション

- ログの証跡の定義について整理するのがよい
- ログを管理する仕組みは以下3つに分類して整理するのがよい。
- 誰でも不正できてしまう状態（ただログを取っているだけ）、②第三者が不正できない仕組み、③本人が不正できない仕組み
- クラウド環境におけるフォレンジックは実施出来ないのが現状。
- クラウドセキュリティに関する有識者を紹介するので話を聞くのがよい

3.3.7　第 7 回検討会（2012.3.29）の概要

○　外部委託調査　報告（株式会社ディアイティ　青嶋　信仁氏、山田　英史氏）
- 詳細は、本報告書「3. 情報収集業務の概要」を参照。

○　クラウド有識者との意見交換結果
- 主に米国で活動されており、米国および日本のクラウドビジネスに精通。
- （意見交換内容）（特にログ・証跡・セキュリティ関連について抜粋）
- 米国では、クラウドビジネスの勝者（Amazon 等）がはっきりしている。
- データの保管場所を明確化する等、セキュリティ面をアピールポイントとするクラウド事業者が増えてきており、この傾向は続くと考える。
- ログや証跡がとれる、ということを明確にしているクラウド事業者は知らない。
- HaaS, PaaS 等、すべてユーザが管理するようなサービス形態では、ログや証跡が 100%とれるだろう。
- 日本では、まだクラウドビジネスの勝者というものがはっきりしていない。業界団体等でクラウドセキュリティを標準化し、これを普及させることは米国と比べ容易と考える。

○　「すぐに実施可能な推奨対策」の取りまとめ
- 詳細は、本報告書「4.2　すぐに実施可能な推奨対策」を参照。

○　次年度以降の課題の検討
- 詳細は、本報告書「4.3. 今後の課題、方向性」を参照。

4. 情報収集業務の概要

4.1 情報収集業務の調査項目

本検討会における議論の参考とするため、平成 24 年 2 月～3 月の期間において、株式会社ディアイティに業務委託を行い、(「平成 23 年度 政府機関における証跡管理の在り方の検討に係る情報収集業務」)、下記の(ア)～(エ)の項目に関する情報収集を行った。本情報収集業務の結果は、第6回及び第7回検討会の場において報告された。

(ア) 民間企業からの不正アクセス等のヒアリング

組織外部から通信ネットワークを介して組織内部の情報システムに不正アクセスされ、組織内部の情報を窃盗された、もしくは未遂に終わった攻撃事例について、取得していたログ・証跡を調査し、それらが攻撃防御や事後調査等にどの程度有効であったかについて調査する。具体的には、ログ・証跡を取得していた機器(ファイアウォール・IDS・データベースサーバ等)毎に、どの種の情報(アクセス元情報・イベント情報等)を記録しているか、また、それらの費用概算等について調査する。

作業方法:外部組織に組織内部の情報を窃盗されたまたは未遂に終わった経験を持つ政府機関や企業を選定し、アンケート又はヒアリングにより選定した組織が行っていたログ・証跡管理方法等について調査する。併せてそれらの費用概算等も調査する。

結果まとめ:各調査対象組織と調査についてまとめ、考察する。

(イ) ログ・証跡管理に関する製品及びサービス調査

ログ・証跡の取得及び分析に係る市販製品及びサービス内容を調査する。市販製品の調査については、製品毎に、概要(製品名、ベンダー、製品種別、価格等)、取得できるログ・証跡の情報(アクセス元情報・イベント情報等)、ログ・証跡解析の内容(解析により分かること、解析方法等)等を調査する。また、サービスの調査については、サービス毎に、概要(サービス名、サービス提供社、価格等)、契約形態(期間契約、スポット契約)、提供サービス内容(窃盗された情報の特定、攻撃元特定に資する情報の抽出、不正アクセス痕跡の定常監視等)等を調査する。

作業方法:ログ及び証跡の取得及び分析に関わる市販製品及びサービスをインターネット等により洗い出し、公開情報をベースに概要、取得できるログ・証跡内容、ログ・証跡解析内容、提供サービス内容、契約形態等を調査する。不足情報は製品等の開発・販売元に問い合わせ補完する。

結果まとめ:各調査対象製品・サービスと調査項目を対応させた表形式に整理する。表に加え特記事項についてコメントする。

(ウ) ログ・証跡管理に関する報告書の調査

セキュリティ製品及びサービス提供会社が公開し現在入手可能な、ログ・証跡の管理及び解析に係る報告書を収集するとともに、各報告書の概要を記載した一覧を作成する。

作業方法:セキュリティ製品及びサービス提供会社が公開するログ・証跡の管理・解析の報告書をインターネット等により洗い出し、公開情報をベースに報告書の概要を調査する。

結果まとめ:ログ・証跡の管理・解析の報告書の概要を一覧にまとめる。

（エ） 海外政府機関およびそれに準ずるログ・証跡管理に関わる報告書やガイドラインの調査

海外政府機関及びそれに準ずる機関が公開し現在入手可能な、ログ・証跡の管理及び解析に係る報告書やガイドライン等の公開文章を収集するとともに、各報告書の概要を記載した一覧を作成する。

作業方法:海外政府機関及びそれに準ずる機関のログ及び証跡に関する報告書やガイドラインについてインターネット等により洗い出し、公開情報をベースにそれらの概要を調査する。

結果まとめ:ログ・証跡の管理・解析に関する報告書やガイドラインの概要を一覧にまとめる

4.2 （ア）民間企業からの不正アクセス等のヒアリング結果

4.2.1 ヒアリング対象の選定

新しいタイプの攻撃の対象とされやすいと思われる重要インフラ業種 9 社（情報通信、金融、航空、鉄道、電力、ガス、医療、水道、物流）に、ヒアリングの趣旨と内容を記載した資料を送付し、ヒアリングへの協力を依頼したところ、そのうち 5 社がヒアリングに応じた。

4.2.2 ヒアリング項目及び方法

ヒアリングの対象としたログは、Firewall、Proxy、Router など Gateway 関係の機器や Server や PC などが記録しているものと、ネットワーク上の通信データ自体とした。

ヒアリングは委託調査会社が中心となり実施した。4 社のヒアリングでは、内閣官房情報セキュリティセンターも同行した。ヒアリング対象会社によってヒアリング内容に差異がでないよう、全てのヒアリングは同一の者が実施した。ヒアリング時間は概ね 1 時間とした。（2012 年 2 月 16 日～3 月 8 日）

4.2.3 ヒアリング結果概要

全てのヒアリング対象会社においては、組織外部から通信ネットワークを介して組織内部の情報システムに不正アクセスされ、組織内部の情報を窃盗された、もしくは未遂に終わった攻撃事例は「無い」との回答であった。よって、ヒアリング前に想定していた、それらをもとにしたログ・証跡の有効性についての情報は得られなかった。よって、現状のログの取得状況や活用などについてもヒアリングを行った。

Gateway 関係の機器の運用管理は、外部に委託しているヒアリング対象会社が多く、自社でログの詳細について把握しているところはあまりなかった。外部委託先のサービスにおけるログの監視体制をヒアリングしたところ、IPS/IDS のリアルタイム監視や Firewall や Proxy の運用管理を行っているレベルであり、ログの監視等を行っているケースはほとんど無かった。

クライアント PC の操作ログの収集・管理については重視されていた。社内にある機器については、ログ収集管理ツールを使って取得はしている場合もあるが、多くの場合、各機器のデフォルト設定で動作している。

ログ収集・管理に関する意識として多いのは、内部統制および機器に異常がおきたときの参照情報としての活用であり、サイバー攻撃への対応などは外部委託への依頼という位置付けが多かった。

今後の予定についても、IPS/IDS や通信データ保存などの通信データの活用は想定していても、各機器の

ログを積極的に活用しようというところは少なかった。

4.2.4 ヒアリング結果詳細

以下にヒアリング結果の詳細を示す。なお、ヒアリングにおいては、ヒアリング対象会社が特定できないことを条件に実施したこともあり、各ヒアリング対象会社の特徴や所属業界による分析結果等は掲載していない。

I. 情報の窃盗、窃盗未遂等の状況

社外から社内への不正アクセスにより、社内の情報を窃盗された、もしくは、窃盗未遂が起きた事実の有無と、その際のログの活用状況についてヒアリングした結果、全てのヒアリング対象会社において、窃盗ないし窃盗未遂の事実を確認していない、との回答であった。

なお、一部のヒアリング対象会社においては、目的が社内の情報の窃盗であるかは判断できないが、下記のような不正アクセスと思われる攻撃が確認されている。

- ○ メールの添付ファイルに実行ファイル（国外 C&C サーバーへ定期的な接続を行う）があった。リアルタイムな検知で判明しただけで、調査にログは使われていない。
- ○ OpenSSL の脆弱性をつく攻撃があった。リアルタイムな検知で判明しただけで、調査にログは使われていない。

また、多くのヒアリング対象会社から、不正アクセスに関するログの扱いに関して下記のようなコメントがあった。

- ○ Gateway 上でウイルス対策ソフトが防いだ場合もあった可能性があるが、それ自体は社内に入る前に防いでいるため、一般的には確認されていない。よって、実体はわからない。
- ○ IPS/IDS やウイルス対策ソフトのリアルタイムな通知で異常を知るもので、ログを調査して異常を知るところはほとんどなかった。
- ○ ログはリアルタイムな通知で異常がわかった後で見直すことがあるというもので、常時利用してはいない。

II. 対策として導入したツールや設定した項目

近年のサイバー攻撃の高まりを受け、セキュリティ対策として最近導入したツールや設定した項目についてヒアリングした結果、下表のような回答が得られた。

目的	対策内容
ログの解析時間を短縮	・ 高速なログ検索ツールの導入
不正な通信の発見と遮断	・ IPS の導入
総合的な対策レベルの向上	・ ウイルス対策会社の最上位サービスの利用 ・ 特定のセキュリティ対策製品を会社にこだわらずに機能毎に強い製品に入れ替え
不正なサイトへのアクセス遮断	・ Web レピテーション機能を有する製品の導入

通信データの取得・解析	・ 通信データ取得装置の増設 ・ 通信アナライザの導入

上記結果のほか、その他のヒアリング状況も加味すると、近年のセキュリティ対策の概況として下記のような状況であることが推測される。

○ 通信の記録や監視の強化が実施されている。
○ ログの収集・管理を強化するという動きはあまりない。
○ どのような対策が有効であるかが不明であるが、既存のセキュリティ対策で不十分と思われる箇所を推測し、その箇所を補う機器等を順次導入している。

III. ログ収集・管理に関連し導入や開発を希望する機能や製品

ログ収集・管理に関連し、導入や開発を希望する機能や製品についてヒアリングした結果、下記のような回答が得られた。

○ 複数機器のログを収集し、相関的に解析してレポートを表示できる製品。
○ Proxy が複数段ある場合でもログを連携させて組織内 PC の IP アドレスが特定できる製品。
○ 2 バイトコードに対応したログ管理ツール。海外の製品は2バイトコード未対応が多い。
○ IPS/IDS。
○ 通信データ取得ツール。

IV. ログの保存状況

ログの保存状況についてヒアリングした結果、下記のような回答が得られた。

ログ保存期間	対象	ログ保存期間の設定理由
1 ヶ月	GateWay 機器全般	外部委託先の仕様
3 ヶ月	Proxy	HDD の容量の制限
	Web Server	特段の理由はない
1 年	全てのログを対象	特段の理由はない
	ID 管理及び DB Server	特段の理由はない
5 年	Server 全般	特段の理由はない
	ID 管理	特段の理由はない

上記のほか、下記のようなヒアリング結果も得られた。

○ 新しいタイプの攻撃等の増加を理由にログの保存期間を延ばしたというところはない。
○ 外部委託業者へ任せている場合、ログの保存期間を知らない場合が多い。
○ ログの改ざん対策については、ログ収集ツールの機能を利用している。ログ収集ツールを導入していない場合で、ログの改ざん対策を行っているケースはない。

V. ログ収集・管理等に関係する費用

ログ収集・管理等に関係する費用についてヒアリングした結果の概況は下記の通り。

- ○ Gateway 関係についてのログ管理は外部委託が多いが、その費用や具体的なサービス名・内容は秘密が多く把握できていない。
- ○ 外部委託費用を除くと、多いところで月額 100 万円との回答があった。

VI. 利用しているログ管理ツール

利用しているログ管理ツールについてヒアリングした結果の概況は下記の通り。

種類	製品名	開発会社
ログ収集及び検索ソフト	ArcSight	ArcSight
	LogStorage	インフォサンエンス
	快速サーチャーLogRevi	インテック
	Splunk	Splunk
クライアントログ中心	CAT6	LanScope
	SeP	ハミングヘッズ
	SCOM	Microsoft
	SKYSEA	Sky
	ManagementCore	M/Core
通信データ取得機器	PacketBlackHole	ネットエージェント

上記のほか、下記のようなヒアリング結果も得られた。

- ○ クライアントログ中心のものは、サイバー攻撃等を意識したものではなく、内部統制のための導入目的が主である。

4.2.5 その他ヒアリング全体に関する所感（作業委託発注会社によるもの）

サイバー攻撃自体を想定した防御は外部専門業者任せが多く、専門家は社内には少ないことがわかった。また、社内の情報が狙われていること自体への危機意識は、システム（導入ツール）で分からなければ仕方がないというレベルであり、あまり高くないと感じられた。

ヒアリングされる会社側の意見としては、標的型攻撃なども定義や公開が不十分な状態（内容が難しすぎるといった点を含む）であり、そもそも、それら自体の理解ができていない。解析手順などが定義されていればよいが、それらもなく、「専門家がいない」中、それらに対応することはできない。よって、標的型攻撃を意識した解析などはできないし、回答もできないというものであった。

ここから分かることとしては、ログ関係の導入および運用を進めていった場合でも、「専門家がいない」状況を合わせて改善していかないと、状況に合わせた効果的なログの設定や、いざという時の活用を行うことは難しい、ということであった。

4.3 （イ）ログ・証跡管理に関する製品およびサービス調査結果

4.3.1 調査方法

ログ・証跡管理に関する製品およびサービスについて、Web 検索や雑誌記事等により一次選定を行った。その後、製品開発会社またはサービス提供会社に資料請求を行い、可能な範囲でヒアリングによる詳細調査を行った。

4.3.2 調査対象製品・サービス

調査対象とした製品・サービスおよび、ヒアリングの実施有無は下表の通り。

カテゴリ	製品・サービス名	ヒアリング実施有無
ログ統合管理ツール	RSA enVision	○
	Logstorage	○
	AnalyticMart for LogAuditor	○
	快速サーチャーLogRavi	○
	LogStare Tetra	―
	ArcSight ESM	―
	splunk	―
ネットワーク監視ツール	RSA NetWitness	○
	PacketBlackHole	○
	NetDetector	○
サーバアクセス監視ツール	Alog ConVerter	○
	VISUACT	―
	File Server Audit	○
クライアント操作監視ツール	MylogStar	○
	LanScope CAT	―
	CWAT	―
サービス	(株)ラック／セキュリティ監視・診断サービス	○
	(株)インフォセック／InfoCIC	○
	(株)JIEC／Log Shelter	―
	(株)日立システムズ／SecureEagle/SIM	―

4.3.3 調査項目

調査項目は下表の通り。

カテゴリ	調査項目	
	大分類	小分類
ログ・証跡管理製品	製品構成（プラットホーム、アプリケーションの種類など）	－
	ログ収集機能	収集対象（OS、DB、ネットワーク機器、等）
		収集内容（アクセス元情報、イベント情報、等）
		エージェントの有無
	ログ保管機能	保管容量
		圧縮、暗号化
		ログ原本の保管の可否
		ログへのアクセス制限
	ログ解析機能	解析方法（相関分析等）
		テンプレートの有無
	レポート機能	ログ解析レポートの内容
		テンプレートの有無
	導入コスト、契約形態	ログ・証跡管理サービス
サービス	提供サービス内容（窃盗された情報の特定、攻撃元特定に資する情報の抽出、不正アクセス痕跡の定常監視等）	－
	導入コスト	－
	契約形態（契約期間、スポット契約）	－

4.3.4 調査結果

別紙 1 に製品調査結果を、別紙 2 にサービス調査結果を記した表を記載する。

その他、調査を通して得られた情報は下記の通り。

- ○ ログ統合管理ツールの導入事例の多くは内部統制目的（操作の正当性の裏付け）が主で、セキュリティオペレーション目的は少ない。（特に統合管理ツールで）。
- ○ ログ統合管理ツールは、検索速度が重視される傾向にある。既存のシステム環境にログ統合管理ツールを導入し、各システムに蓄積されたログを収集し集計するというのは、非常に負荷の高い処理であるため。
- ○ 解析機能は、ネットワーク監視ツール、サーバ監視ツール、クライアント監視ツールの方が統合管理ツールよりも充実している。統合管理ツールは、異なった複数のログを同じ様式で時系列に相関分析することが主体。
- ○ 多くの事例では、ネットワーク監視ツール、サーバ監視ツール、クライアント監視ツールを適所に配置し統合管理ツールと連携している。
- ○ 解析機能を有効に利用するには、ポリシーを上手く定義する必要がある。標準的な業務手順を定

め、それを基準に逸脱行為を監視する使い方が有効だが、業務手順の整備という面倒な作業が伴う。

○ 各製品で解析機能に特徴があるが、例えば標的型攻撃かどうかを見極めるのは、出力結果を読み取る者の知見に依存する。

4.3.5 備考：ログ・証跡管理製品・サービスを比較するポイント

調査を通して、ログ・証跡管理製品及びサービスを調査・比較する際のポイントが明らかとなったので、調達等における参考として下記に整理する。

・ ログ・証跡管理製品

項目			調査・比較する際のポイント
製品のプロフィール	開発元／販売元		・ 開発国（国産／海外製品）。 ・ 開発元の実績・安定性。 ・ 日本語対応の程度（海外製品の場合。メニューの言語表示、データ再現が 2 バイト対応か、等。）。
	製品構成		・ アプライアンス／ソフトウェア ・ 構成要素（収集ユニット、保存ユニット、分析ユニット、管理コンソール等）とそれぞれの役割
	動作環境・条件		・ ソフトウェア製品の場合、構成要素それぞれのプラットホーム（ハードウェア／ソフトウェア）のスペック
製品の機能	ログ収集機能	エージェント	・ エージェントの有無。エージェント不要としていても、ある条件ではエージェントを必要とするものがある。
		収集対象	・ 収集対象とする装置の種類及び機種。（製品によっては入退室管理、監視カメラ画像も対象となるものがある。） ・ 収集対象とする装置側に実装すべき条件。 ・ 対応プロトコル（Syslog、SNMP 等）。 ・ 対象ログ（Windows 監査ログ等）。 ・ 連携製品の種類。（既存のログ管理システム等との連携可否）
	ログ保管機能	保管先	・ 具体的な保管先。DB に保管される場合は DB の種類。
		保管容量	・ 保管容量の上限と増設方法。 ・ 最大容量の実績。
		圧縮	・ 圧縮率と要件。 ・ 圧縮対象（生ログを圧縮／インデックス化したものを圧縮）。
		暗号化	・ 暗号化の有無、使用する暗号アルゴリズム。
		生ログ保管	・ 生ログの保管の可否および保管場所。 ・ ログ収集後に対象装置上におけるログの削除有無。
		ログへのアクセス制限	・ ログへのアクセス制限方法。 ・ ログ改ざん検知方法（ハッシュ、電子署名等の利用）。

	ログ解析機能	監視機能	・ 監視の条件定義方法、及び、定義可能な内容。 ・ アラート受信方法。
		解析機能	・ 検索速度。特に大量のログを扱う場合には重要。 ・ ログフォーマット。（製品によって差異が大きい。各種ログを統一様式に時系列に整理するものやユーザの操作とログをひも付けて整理するもの等がある。） ・ 相関分析、分析ロジック。 ・ 検索および解析条件の設定内容や設定方法。（製品によって差異が大きい。） ・ 分析用テンプレート。（内部統制用のものが多いため、標的型攻撃を意識したカスタマイズが可能かどうかは確認が必要。）
		レポート機能	・ 表形式、グラフ形式。 ・ 特徴的なレポート項目。（特定のユーザの動線に沿って表示する等） ・ 出力フォーマット（CSV、PDF 等）。
契約形態			・ ライセンス体系。 ・ 保守条件。 ・ 導入支援等サービスの有無。
コスト			・ 初期導入コスト ・ ランニングコスト。

・ ログ・証跡管理サービス

項目		調査・比較する際のポイント
サービスのプロフィール	開発元／販売元	・ サービス提供会社の国籍（国内／海外（外資）） ・ サービス提供会社の実績・安定性 ・ ログデータの保存場所。特に海外サービスの場合に留意する。 ・ 日本語による支援の可否。特に海外サービスの場合に留意する。
	サービスの概要	・ サービスの全体構成。特にユーザ側に設置する装置の有無。 ・ サービスの内容。
サービス内容	不正アクセス痕跡の定常監視	・ 監視対象装置、監視対象ログ。 ・ 監視時間の条件。24 時間 365 日リアルタイムでない場合がある。 ・ 監視ポリシー。 ・ アラートの内容。 ・ アラートの受信方法。
	窃盗された情報の特定	・ ログその他の情報による分析方法。 ・ 窃盗された情報の特定方法。

	攻撃元特定に資する情報の抽出	・ ログその他の情報による分析方法。 ・ 攻撃経路、攻撃手法の特定方法
	その他	・ ログをセンター側に保存する場合は、センターまでのネットワーク経路の安全対策、保管ログへのアクセス制限方法。
契約形態等	契約形態	・ 標的型攻撃を対象とした場合のオプション。 ・ 契約期間(年間、月毎等)。
	導入コスト	・ 初期費用。 ・ 月額サービス費用。

4.4 （ウ）ログ・証跡管理に関する報告書調査結果

4.4.1 調査方法

Web 検索、ログ管理製品・サービス事業者へのヒアリング、ユーザ企業へのヒアリング等により、ログ・証跡管理に関する資料の調査を行った。

4.4.2 結果

新しいタイプの攻撃に関し、主にログ・証跡管理に着目した報告書ならびに技術資料の調査を行った。なお、調査対象はいずれも非公開前提の資料で内容も機密性が高いものであったため、本報告書では調査結果は記載しない。

4.5 （エ）海外政府機関及びそれに準ずるログ・証跡管理に関わる報告書やガイドラインの調査結果

4.5.1 調査方法

Web 検索により、海外政府機関及びそれに準ずるログ・証跡管理に関わる報告書やガイドラインの調査を行った。

4.5.2 結果

別紙 3 に調査結果を記した表を記載する。

（以上）

【別紙1】ログ・証跡管理に関する製品

製品のプロフィール	製品種別		ログ統合管理ツール	ログ統合管理ツール	ログ統合管理ツール
	製品名		RSA enVision	Logstorage	AnalyticMart for LogAuditor
	開発元／販売元		米EMC／EMCジャパン	インフォサイエンス／アシスト他	三菱電機中央研／三菱電機インフォメーションテクノロジー
	製品構成		アプライアンス	ソフトウェア	ソフトウェア LDB: ログ管理DB(検索専用) RSF/DSF: ETLツール AAS: AQL DBへのデータ投入ツール AQL: DB ※ 個々のソフトウェアは単品で購入可
	動作環境・条件		—	・Windows Server 2003/2008 ・RedHat Linux / CentOS ・Solaris (x86, SPARC)	Windows Server 2008
製品の機能	ログ収集機能	エージェント	無し	エージェント、ツール、エージェントレス各種	ETLツールによるファイル渡し
		収集対象	・対象装置 Windowsサーバ、ファイアウォール、IDS/IPS、DB、SAN/NAS 170種類以上に対応 未対応装置はExcelベースのテンプレートで対応可 ・対応プロトコル Syslog, Syslog NG SNMP テキストファイル(カンマ/タブ/スペース区切り) ODBC (リモートDB接続) XML ファイル(HTTP取得) Windows イベントログ API CheckPoint OPSEC interface Cisco IDS RDEP	・対象装置 Windows、UNIX、ファイアウォール、IDS/IPS、DB、 VM Ware等 未対応装置はExcelベースのテンプレートで対応可 ・対象プロトコル Syslog FTP/FTPS(暗号化FTP) ファイル共有 SNMP Logstorage Agent (リアルタイム収集) EventLogCollector (エージェントレス収集) ・連携製品 CWAT、SecurePrint!、MylogStar、AUDIT MASTER、SecureCube AccessCheck、Auge AccessWatcher、i-FILTER、InfoTrace、監査れポータル、ARCACLAVIS Revo、PISO、LanScope Cat、File Server Audit、VISUACT、Chakra、SecureSphere等 約20種	・対象装置 Windows、UNIX、ファイアウォール、IDS/IPS、URLフィルタリングDB、仮想環境、入退室管理、監視カメラ画像等 ・連携製品 ALog ConVerter、File Server Audit、Chakra、CWAT、InfoTrace、IPLocks、PISO、VISUACT、K5100、SSDB監査、監査れポータル、myB3smarte等
	ログ保管機能	保管先	本体内: LogSmart IPDB(独自DB)	プラットホームのHD上	独自追記型DB
		保管容量	標準300GB、外付けHDで増設可	制限無し(130TB/年の実績あり)	制限無し
		圧縮	○(生ログを最大94%圧縮)	○(1/10)	○(1/10)
		暗号化	○	○	×
		生ログ保管	○	○	○
		ログへのアクセス制限	ID/パスワードによるアクセス制限	ID/パスワードによるアクセス制限 ハッシュによる改ざん検出	追記型方式で改ざんリスク減 ID/パスワードによるアクセス制限
	ログ解析機能	監視機能	・SANS Top20等に照らしたインシデント検知、リアルタイムアラート発信 ・特定ファイルへのアクセス、特権利用等の監視により、ポリシー違反の検知	ログの発生頻度、シナリオに基づいた検知によるアラート発信(メール送信／SNMP Trap／外部コマンド実行)	不正アクセス検知テンプレートにより検知とアラート発信
		ログ解析機能	・イベントおよびデータ内容の検査 ・相関分析(テンプレート200種以上) ・ベースライン分析	・Windowsイベントログをユーザの操作とログのひも付で整理 ・and/or条件による検索 ・全ログの横断追跡、ログ全体の兆候分析 ・連携製品については1製品あたり、20種類程度のテンプレートを提供 (トータル300種以上) ・GUI画面を利用し、ユーザによるテンプレートの作成も可能。	・独自OSによる高速検索 ・各ログを横断的にキーワード検索(特定の人物の振る舞い追跡等) ・テンプレート提供(200種以上) ・条件の変更はできるがテンプレート自体は変更不可
		レポート機能	・ガイドライン等(PCIDSS、SOX、…)に沿ったテンプレート2,000種以上 ・管理用ソフトウェアEvent Explorer(Windowsマシンに実装)によるインシデント管理とダッシュボードによる可視化	・検索機能、集計機能、検知機能で保存された各条件をレポート形式で出力 ・標準形式のレポートをカスタマイズ可能 ・リソース使用状況の把握、申請データと作業ログの突合、部署・社員マスタとアクセスログの連携、クライアントPC 利用時間の分析等の表・グラフ表示	・蓄積したログから組織別、日付別、イベント別など多次元分析レポートを行うためのExcelアドインを標準装備 ・ウィザード形式により非定形分析を容易にし明細表示や統計グラフ表示を行う
契約形態等	契約形態	ライセンス・保守等	エントリーモデルES560から始め、ライセンスの追加のみで対応デバイス数、ディスク容量の拡張に対応。	初年度から保守費発生(任意) 保守費: ライセンス費用の20%	LDB、RSF/DSF、AA、AQLは単品で購入可 初年度から保守費発生(任意) 保守費: 製品の15%
	導入コスト		約680万円～	ワークグループ版(基本パッケージ) 65万円 ・コンソールサーバ 1台、LogGate 1グループ、EventLogCollector(エージェントレス ログ収集ツール)、エージェント 制限無し	900万円～ LDB単品: 260万円 AQL単品: 460万円

【別紙1】ログ・証跡管理に関する製品

製品のプロフィール	製品種別		ログ統合管理ツール	ログ統合管理ツール	ログ統合管理ツール
	製品名		快速サーチャーLogRavi	LogStare Tetra	ArcSight ESM
	開発元／販売元		(株)インテック／(株)アイ・アイ・エム他	(株)セキュアヴェイル	米ArcSight／SCSK等
	製品構成		ソフトウェア	ソフトウェア	アプライアンス／ソフトウェア
	動作環境・条件		サーバ: Windows Server 2003、2008 クライアント: Windows Server r 2003、2008 Windows XP、Vist、7	Red Hat Enterprise Linux 5 Server	管理ソフト: RedHat Linux, Windows Server 2003、IBM AIX 5L 5.3、Solaris 9/10
製品の機能	ログ収集機能	エージェント	○	無し	無し
		収集対象	・FTP、ファイルコピーでログ収集、Windowsイベントログをエージェントで取り込み、Syslogはオプション KIWI+で取り込み ・対象装置 Windows、UNIX、Active Directory、ファイアウォール、IDS/IPS等 ・対象ログ PC操作/アクセス管理/情報・資産管理、DB/ファイルサーバー、OS/ホスト/アプリケーションサーバ、ディレクトリ/IDM/認証、CRM/ERP/SCM/SFA、プリントサーバー、ポータル/グループウェア、ネットワーク関連、運用管理 ・連携製品 iNetSec Smart Finder、JP1、TRAVENTY SuperVision、LanScope Cat6、InfoTrace、QOH、MylogStar、ALog ConVerter、File Server Audit、VISUACT、PISO、Chakra、iSecurity、Auge Access Watcher、SmartOn、結人／束人、LDAP Manager4、InterSafe SecureDevice、ProActive、TASKGUARD、KIWI Syslog Server、F3等	・対象装置 ファイアウォール、スイッチ、プロキシ、Webサーバ、メールサーバ、ファイルサーバ、DB ・対象ログ テキスト形式のログであれば全て一元集約可能、またWindowsログオプションでWindowsログの収集も可能 ・収集方法 FTPによる受信、Syslogによる受信、 SCP/FTP/HTTP(S)による取得、 MOVEやCOPYによる取得 ・連携製品 VISUACT、PISO、SecureCube/PC Check等	・対象装置 Windows、UNIX、ファイアウォール、IDS/IPS、ルータ、DB、脆弱性検査装置、認証装置、ウイルス検知装置、入退室管理等 ・対象ログ 300種類以上のログフォーマットに標準対応
	ログ保管機能	保管先	サーバ上の独自DB	サーバ上	ArcSight DB
		保管容量	制限無し	制限無し	
		圧縮	○(1/10に圧縮)	○	○
		暗号化	○	○	×
		生ログ保管	×	○	
		ログへのアクセス制限	部署別等グループ権限設定 ID/パスワードによるアクセス制限	ID/パスワードによるアクセス制限 改ざん検出	ID/パスワードによるアクセス制限
	ログ解析機能	監視機能	重要データへのアクセス違反、システムエラー等をアラート発信 部門毎、管理者のみ等送信先を選択可	・10分に1回、事前に定義されたポリシーを基準にログのモニタリングを行い、異常を検知を管理者へ通知 ・アラート結果は、履歴情報としてLogStareへ保存 ・条件例 Syslog キーワード条件: 管理者変更ログ、リンクダウンログ、ログイン失敗等 正常時のログファイルサイズの閾値より小さいものや大きいもの	・監視分析ルール、レポートテンプレート合計350種類以上 ・収集した情報を正規化し、ルール設定によりインシデントをリアルタイムで検知 収集したログから条件にマッチする情報をリアルタイムで監視、通知 収集したログの相関関係をリアルタイムで監視
		ログ解析機能	・独自DBによる高速検索 ・特定ユーザの動線のタイムライン分析 ・複数ログの突合せ相関分析	・基本サマリ分析: 事前に定義した項目内容に毎日自動分析され、グラフや表でわかりやすくシステムの利用状況を可視化 ・クローズアップ分析: 基本サマリ分析(傾向分析)やポリシー違反検知機能で発見された「普段と異なるログ」をピックアップし問題を特定 ・ピンポイント分析: ログ分析対象が明確な場合、検索条件を指定してダイレクトにログを抽出 ・基本サマリ分析→クローズアップ分析→ピンポイント分析と分析を進行して問題を特定	・ユーザID と組織内の役職や業務内容、アクセス権減の相関分析 ・サーバなどと、動的に割り当てられたIP アドレスとの関連付けによるネットワークログ相関分析 ・企業内システム、ネットワーク監視システムなどのイベントと、IP アドレス上のイベントを関連づけロケーション情報の相関分析 ・IDS やファイアウォールなどで起こったイベントの値を組み合わせて相関分析し攻撃を検出 ・特定システムのインシデントが組織のどの部分に影響を受けるかを割り出し
		レポート機能	・クライアントソフトによるダッシュボート表示 ・複数ログ専用ビューア表示 ・レポート毎のアラート発生数、推移、傾向の表示 ・標準テンプレート(カスタマイズ可能)	・WebUI上の操作で、マウスで必要な項目を設定してオリジナルなサマリレポートを作成 ・基本サマリレポートに登録された全てのレポート項目およびクローズアップ分析やピンポイント分析の結果に表紙と目次を付加し、一冊の報告書としてPDF出力	・監視分析ルール、レポートテンプレート合計350種類以上 ・収集したログから統計情報を作成し、グラフィカルに表示 ・収集したログから条件にマッチする情報をリアルタイムで監視、通知 ・指定した項目、指定した期間、指定した集計方法にてレポートを出力 ・スケジュール機能による自動作成機能 ・多彩な出力方式(PDF、HTML、CSV、TXT、RTF、XML)
契約形態等	契約形態	ライセンス・保守等	初年度から保守費発生(任意) 基本ライセンス保守費: 25.5万円	初年度から保守費発生(任意) 基本ライセンス(5ノード)保守費: 39,600円 ※ ログ調査チケット(有料)制あり	
	導入コスト		基本ライセンス: 170万円 定義エディタライセンス: 98万円 同時処理ライセンス: 100万円 突合せレポートライセンス: 50万円　その他	基本ライセンス: 198万円(5ノード) 分析レポート拡張モジュール: 78万2000円(1アプリ) Windowsログオプション: 25万8000円(1 Windows server)	300万円～

【別紙1】ログ・証跡管理に関する製品

製品のプロフィール	製品種別		ログ統合管理ツール	ネットワーク監視ツール	ネットワーク監視ツール
	製品名		splunk	RSA NetWitness	PacketBlackHole
	開発元／販売元		米Splunk／マクニカネットワークス他	米EMC／EMCジャパン	ネットエージェント／日本コムシス他
	製品構成		ソフトウェア	・パケット収集製品群 ・Decoder（アプライアンス） ・Concentrator（アプライアンス） ・Broker（アプライアンス） ・パケット解析製品群 ・Spectrum（アプライアンス） ・Informer（アプライアンス） ・Inverstigator（ソフト：Windowsマシンに実装）	アプライアンスまたはバーチャルアプライアンス
	動作環境・条件		・インデックスサーバ Solaris9,10、Linu、Free BSD 6.1, 6.2以降、 Windows server 2003, 2008、Windows XP 、Vista MacOSX 10.5, 10.6、AIX 5.2, 5.3, 6.1 HP - UX 11	―	―
製品の機能	ログ収集機能	エージェント	無し（専用エージェントもあり）	無し	無し（プロミスキャスモードの場合）
		収集対象	・ログファイルが保存されているディレクトリへのマウント、クリプトファイルの実行および専用エージェントによるログ収集 ・対象装置と対象ログ Windows：レジストリ、イベントログ、ファイルシステム、システムログ Linux/Unix：コンフィグファイル、Syslog、ファイルシステム、ps、iostat、top 仮想／クラウド：Hypervisor、ゲストOS、Apps、Cloud アプリケーション：Web logs、Log4J、JMS、JMX、.NET events、Code and scripts DB：コンフィグファイル、監査／クエリログ、テーブル、スキーマ ネットワーク機器：コンフィグファイル、Syslog、SNMP、netflow	・対象パケット HTTP、FTP、TFTP、TELNET、SMTP、POP3、NNTP、 DNS、SOCKS、HTTPS、SSL、SSH、Vcard、PGP、SMIME、DHCP、NETBIOS、SMB/CIFS、SNMP、NFS、 RIP、MSRPC、Lotus Notes、TDS (MSSQL)、TNS、 IRC、Lotus Sametime、MSN IM、RTP、Gnutella、 Yahoo Messenger 、A IM、SIP 、H. 323 、Net2 Phone 、Yahoo Chat、SCCP、Bittorrent、GTALK、Hotmail、Yahoo Mail、GMail、TOR、Social Networking、Fast Flux、VLANタギング等 ・パケットの収集 各所に配置したDecoderでパケットを収集しメタデータを付与 Concentratorがメタデータのみをを Decoderから収集（Brokerにより複数のConcentratorのデータを集約）	・収集対象 PacketBlackHoleを接続しているIDSハブや、ポートミラーリング設定しているネットワーク機器に流れるパケットデータ、及び、https通信 ・収集内容 ネットワーク機器に流れるlayer2データ全てを保存、https通信も保存
	ログ保管機能	保管先	インデックスサーバ上	パケットはDecoderに保管 メタデータはConcentratorrに保管	本体HD上
		保管容量	制限無し	Decoder： 2TB冗長～ Concentratorr： 12TB冗長 他 両製品共、容量はモデルにより変動	1ユニットあたりの保管容量は1TB～46TB スケールアウトすることで無制限
		圧縮	○（1/10）	○（メタデータは全パケットキャプチャの10%）	○
		暗号化	×	×	×
		生ログ保管	○	生パケットはDecoderに保管	○生パケット保管
		ログへのアクセス制限	ID/パスワードによるアクセス制限	ID/パスワードによるアクセス制限	ユーザ認証、及び、指定端末からのログインのみを許可するなどの制限
	ログ解析機能	監視機能	・柔軟な条件、スケジュール・しきい値設定 ・リアルタイムアラート ・アラートコンソールによる一覧表示 ・メール通知、スクリプト実行など	・Spectrumによるパケット解析による不審なセッションの発見と通知 ・ファイル構文分析（File属性／ヘッダ） ・ファイルの流入経路や流入方法 ・既知の脅威情報とのマッチング ・仮想環境（SandBox）上での実行確認	イベント抽出と定型検索
		ログ解析機能	・検索BOXにキーワードや専用コマンドを入力して情報抽出 ・キューIDなどをキーにして、多段構成のメールサーバのログを横串検索し、メール配信ステータスを即座に把握可能 ・複数のデバイスからログを収集し、異なるキー情報を紐付け、システムの横断的な相関分析調査が可能	・Spectrumによるパケット解析（上欄参照） ・保管されたパケット（Web、メール、音声、ファイル等）の再生確認	・定型検索 ・全文検索 ・国別抽出 ・保管されたパケットを再生（メール、Webメール、Web、FTP、ファイル、画像、JAVAの再現）
		レポート機能	・検索結果を元にグラフ・レポート作成 ・レポートを元にダッシュボード作成 ・スケジュールによる自動レポート生成 ・メール等による定期配信（PDF他） ・リアルタイムレポート	・Informerによるダッシュボード、チャートの表示 ・Informerによるイベント、アラートのSNMP、Syslog、SMTP等による通知と既存ネットワーク管理製品との連携。 ・Spectrum、Informerの操作、表示はInverstigatorで行う	・件数リスト表示やグラフ表示を行う メール件数、メールIPアドレス、SMTP送信者、受信メール件数、メール通信量、メールレコード数 Webアクセス件数、検索件数、Webメール件数、Webヒット数 TCP通信件数、TCP通信量、TCPレコード FTPファイル数 Oracleアカウント、Oracleクエリサイズ、Oracleレスポンスサイズ、Oracle件数、Oracleエラー件数
契約形態等	契約形態	ライセンス・保守等	初年度から保守費発生（任意） 保守費：ライセンス費用の18%	ネットワークワークの規模によりDecoder、Concentratorrなどの設置台数が変動。	保守、及び、ライセンス契約によるメンテナンスサポート スタンダードモデル次年度以降保守費：62万円
	導入コスト		198万円～	数千万円規模	スタンダードモデル：264万円（初年度保守含む）

【別紙1】ログ・証跡管理に関する製品

製品のプロフィール	製品種別		ネットワーク監視ツール	サーバアクセス監視ツール	サーバアクセス監視ツール
	製品名		NetDetector	Alog ConVerter	VISUACT
	開発元／販売元		米NIKSUN／SCSK	(株)網屋／日本電気他	セキュリティフライデー／(株)日立情報システムズ等
	製品構成		アプライアンス	ソフトウェア	ソフトウェア
	動作環境・条件		―	Windows 2000、2003、2008 MS SQL Server 2000、2005、2008	Windows server 2003, 2008
製品の機能	ログ収集機能	エージェント	無し	無し	無し
		収集対象	・対象パケット IPパケット(音声、映像、ウェブ、IM、FTP、Eメール、画像等) 鍵情報があればHTTPSも解析可 ・パケットの収集 収集したパケットにメタデータを付与	・対象装置 Windows 2000、2003、2008 ・対象ログ ファイルアクセスログ、ログオンログ、管理者操作ログ、プリントログ、アプリケーション起動ログ、ログオンログ(スクリプト)、ログオフログ(スクリプト)、アクセス権変更ログ	・ミラー対応スイッチやタップを利用し、ファイルサーバに流れるパケットのコピーを取得、パケットからログを生成 ・ログ項目 発生日時、クライアントIPアドレス／コンピュータ名／OS、ユーザアカウント名、サーバIPアドレス／コンピュータ名／OS、メッセージ(詳細は下記参照)、対象リソース / オブジェクト名、接続中の共有名など ・取得メッセージ内容 ログオン／失敗、ログオフ、共有リソース接続、ファイル作成／削除、ディレクトリ作成／削除、ファイルリード／ライト、ファイル／ディレクトリ名のリネーム、ファイル／ディレクトリへの アクセス拒否、サーバ情報取得、ドメインログオン／失敗、Kerberos サービスチケット取得、ファイル／ディレクトリへのアクセス権変更、SMB共有プリンタへの印刷、ファイルのコピー
	ログ保管機能	保管先	本体及びスケジューリングによってFTPサーバにバックアップ	サーバ上	プラットホームのHD上
		保管容量	4TB～160TB以上、外付けHDで増設可	制限無し	制限無し
		圧縮	×	○(1/4000～1/40000)	○(トラフィック 1/1000、イベントログ 1/200)
		暗号化	○	×	×
		生ログ保管	○生パケット保管	×(設定により生ログ保管可)	○
		ログへのアクセス制限	パケット表示、統計表示、設定権限等でアクセス権限を制限 ID/パスワードによるアクセス制限	管理者毎に権限設定 ID/パスワードによるアクセス制限	ID/パスワードによるアクセス制限 スティルス化によりネットワーク経由のアクセスを制限
	ログ解析機能	監視機能	アラートは内部イベントとして保存 関連ソリューションNetVCRにてトラフィック量、レスポンスタイム等のしきい値超過のアラート発信可	ユーザ、ファイル、サーバ、操作等の条件し、条件に合致する場合に管理者へメール通知	ユーザ名、ファイル名、ディレクトリ名とアクションをひも付けて条件設定 メールで管理者に通知
		ログ解析機能	・パケットデータからL2～L4(一部L7)までの統計情報DBを内部で生成し、時間、L2～L4階層等で集計 ・保管されたパケットをコネクション単位で再生(Web、メール、動画、ファイル等)	・イベントログを解析しやすいアクセスログに変換 ・ユーザによるファイルアクセスの成功・失敗履歴を分析 ・ADサーバを対象にした場合：ユーザのWindows認証履歴、特権操作履歴を分析 ・プリントサーバを対象にした場合：いつ、だれが、どのファイルを、何ページ印刷したかを分析 ・アクセス権変更ログ分析	・コピー操作や、コピー/読込時のファイルサイズ出力から、大容量ファイルの個人情報への操作や複数ファイルにまたがる大量技術情報への操作が迅速に追跡可能 ・エクスプローラによってフォルダを開いた時に発生するフォルダ内全ファイルに対するヘッダー読込ログを省略し、またファイルの 分割読込によって発生する複数Readをひとつのログに統合
		レポート機能	検索対象期間、IP等を基に検索し、パケットデータからアプリケーション(メール、Web等)をブラウザを通して再現し表示	・管理コンソールにより集計／監視結果を表、グラフ表示 ・深夜時間帯アクセスランキング、印刷回数ランキング、退職予定者ランキング、重要フォルダへのアクセス等条件に合わせたレポートを	・ダッシュボードによる表、グラフ表示
契約形態等	契約形態	ライセンス・保守等	次年度から保守費発生	初年度から保守費発生(任意) 保守費：ライセンス費用の18%	初年度から保守費発生(任意) VISUACT-HX保守費：36万円
	導入コスト		Fast、Giga、10G Ethernet対応で600万円～6000万円以上(ディスク容量による)	Advance Edition：127万円	VISUACT-HX： 300万円 VISUACT-lite： 10万円／年

【別紙1】ログ・証跡管理に関する製品

製品のプロフィール	製品種別		サーバアクセス監視ツール	クライアント操作監視ツール	クライアント操作監視ツール
	製品名		File Server Audit	MylogStar	LanScope CAT
	開発元／販売元		(株)NSD／キヤノンITソリューションズ他	(株)ラネクシー／NECフィールディング他	エムオーテックス／(株)アイティフォー他
	製品構成		ソフトウェア File server Audit R (集約サーバ) File server Audit Standard (10/100B対応 ファイルサーバ監視) File server Audit Enterprise (GB対応 ファイルサーバ監視) File server Audit DC (ドメインコントローラ監視) ※ File server Audit R (集約サーバ)は大規模構成の場合に導入	ソフトウェア MylogStar Client (監視エージェント) MylogStar Server (管理サーバ) MylogStar Manager (管理コンソール)	ソフトウェア クライアント用エージェント ログを収集/管理用マネージャと ログ閲覧用Webアプリケーション ログ格納用データベース
	動作環境・条件		・File server Audit R : Windows server 2003, 2008 ・File server Audit Standard/Enterprise : Windows server 2003, 2008 ・File server Audit DC : Windows server 2003, 2008	・MylogStar Client : Windows 2000、XP、Vista、7 新クライアント用 Microsoft、Citrix、GraphOn 仮想環境用 Microsoft、VMwar、Citrix ・MylogStar Server : Windows Server 2000、2003、2008 ・MylogStar Manager : Windows 2000、XP、Vista、7	・エージェント Windows 98、NT 4.0、2000、XP、Vista、7 Windows Server 2003/2008 ・マネージャ、Webアプリケーション Windows Serve 2003、2008 ・ログ格納用DB SQL Server
製品の機能	ログ収集機能	エージェント	無し	Client監視エージェント	○
		収集対象	・ミラー対応スイッチやタップを利用し、ファイルサーバに流れるパケットのコピーを取得、パケットからログを生成 ・ログ項目 発生日時、クライアントIPアドレス／コンピュータ名／OS、ユーザアカウント名、サーバIPアドレス／コンピュータ名／OS、メッセージ(詳細は下記参照)、対象リソース / オブジェクト名、接続中の共有名など ・取得メッセージ内容 ログオン／失敗、ログオフ、共有リソース接続、ファイル 作成／削除、ディレクトリ作成／削除、ファイルリード／ライト、ファイル／ディレクトリ名のリネーム、ファイル／ディレクトリへの アクセス拒否、サーバ情報取得、ドメインログオン／失敗、Kerberos サービスチケット取得、ファイル／ディレクトリへのアクセス権変更、SMB共有プリンタへの印刷、ファイルのコピー	・対象端末 Windows 2000、XP、Vista、7 シンクライアント用 Microsoft、Citrix、GraphOn 仮想環境用 Microsoft、VMwar、Citrix ・端末操作ログ ログイン/ログオフ記録、アプリケーション記録、ドキュメント記録、ファイル操作記録、印刷記録、Eメール記録、インターネット記録、FTP記録、クリップボード記録、アクティブウインドウ記録、画面キャプチャ、TCP セッション記録、Windowsイベントログ、Webmail & Messenger(オプション)	・収集対象 Windows PC、Windows server ・収集内容 アプリケーション稼働、操作プロセス、プリント・ログ、Webアクセス
	ログ保管機能	保管先	プラットホームのHD上	MylogStar Serverに保管(SQL Server)	プラットホームのHD上
		保管容量	制限無し	制限無し(SQL サーバの条件16TB)	無制限
		圧縮	○(トラフィック 1/1000、イベントログ 1/200)	×	×
		暗号化	×	クライアント上は暗号化、DB上は平文	×
		生ログ保管	○	○	○
		ログへのアクセス制限	ID/パスワードによるアクセス制限 スティルス化によりネットワーク経由のアクセスを制限	DBへはMylogStar Managerからのみアクセス可 ID/パスワードによるアクセス制限	ID/パスワードによるアクセス制限
	ログ解析機能	監視機能	ユーザ名、ファイル名、ディレクトリ名とアクションをひも付けて条件設定 メールで管理者に通知	設定された検索条件で検索、条件に合致したログを検知し指定されたメールアドレスへアラート発信 メールに警告対象のリストを添付可	・禁止アプリケーションの使用アラート発信 ・キーワード設定で不正なサイトを閲覧禁止、不正サイトのアクセスをアラート表示
		ログ解析機能	・VISUACTと同様に、前後のふるまいから「コピー」アクションが記録できることが特徴 ・CSVで保存された過去のログも検索対象にできる	・AND・OR・NOTを付加し詳細な検索条件が設定可能 ・どのような経路をたどって対象ファイルに行き着いたかを遡って追跡 ・特定のファイルを起点として、その後の取り扱われ方を追跡	・アプリケーションの稼働を数値で把握 ・PCの操作履歴を記録、不正操作の通知・業務時間外操作の把握 ・ネットワークに接続されているプリンタの利用者、出力ファイル名、出力枚数の把握 ・Webサイトの閲覧状況をログ化し、不正なサイトの閲覧を禁止 ・アプリケーションのログオン情報やIDの作成などの入力情報を取得
		レポート機能	・ダッシュボードによる表、グラフ表示 ・オプションの別ソフトで、アクセス総数、アクセスランキングをアクション別、ユーザ別、ファイル別に集計しグラフ表示	・PC利用状況レポート、アプリケーション利用状況、アラーム発生状況等を表・グラフ表示	・Webコンソールで、ネットワークの状態を報告、ネットワーク上の異常の把握、環境の変化を表示 ・Webコンソールでアラートの原因表示 ・3ヶ月間全てのファイルや使用者を細かくトレース ・Webコンソールのレポートを Excelで外部出力
契約形態等	契約形態	ライセンス・保守等	初年度から保守費発生(必須) 保守費: 製品の15%～20%	販売パートナーが導入支援 初年度から保守費発生(任意)	
	導入コスト		File server Audit Standard : 39万6000円～ File server Audit Enterprise : 250万円～	・MylogStar Client : 7,200円／台(年間保守 1,440円) ・MylogStar Server : 48万円(年間保守 96,000円) ・MylogStar Manager : MylogStar Serverに包含	

【別紙1】ログ・証跡管理に関する製品

製品のプロフィール	製品種別		クライアント操作監視ツール
	製品名		CWAT
	開発元／販売元		(株)インテリジェント ウェイブ／NTTアドバンステクノロジ他
	製品構成		ソフトウェア 管理サーバ: オーガナイゼーションモニタ(OM) PC端末ソフト: オペレーションディフェンスコントローラ プロ (OPDC Pro)
	動作環境・条件		・OM Windows Server 2003、2008 SQL Server 2005、2008 ・OPDC Pro Windows XP、Vista、7
製品の機能	ログ収集機能	エージェント	○(OPDC Pro)
		収集対象	・収集対象 Windows PC ・収集内容 ファイル操作、アプリケーション操作、プリント・ログ等
	ログ保管機能	保管先	監査ログ(操作ログ): オペレーションディフェンスコントローラ プロ (OPDC Pro) 警告ログ: オーガナイゼーションモニタ(OM)
		保管容量	無制限
		圧縮	×
		暗号化	×
		生ログ保管	○
		ログへのアクセス制限	ID/パスワードによるアクセス制限
	ログ解析機能	監視機能	・適用するユーザや端末、適用時間・曜日等15の観点でポリシーを設定 ・ポリシー違反の不正操作の情報のみが「警告ログ」としてリアルタイムに監視サーバに送られ、危険度で色分けされて表示 ・ポップアップ画面で、不正操作の詳細表示、オペレーションの中止、管理者へのメール通知等
		ログ解析機能	・ファイルのコピーや印刷、アプリケーションの起動、プリントスクリーン操作、メール送信やWebの操作などを監査ログとして記録 ・管理サーバ(OM)上での監査ログの表示確認 ・管理サーバ(OM)上でのポリシー違反の警告ログの表示確認
		レポート機能	・管理サーバ(OM)上での監査ログの表示 ・管理サーバ(OM)上でのポリシー違反の警告ログの表示、管理者へのメール送信
契約形態等	契約形態	ライセンス・保守等	初年度から保守費発生(任意) 保守費: ライセンス費用の20%
	導入コスト		管理サーバ(OM): 40万円(クライアント100台以下) PC端末ソフト: OPDC Pro 13,000／端末

【別紙2】ログ・証跡管理に関するサービス

サービスのプロフィール	製品種別	ログ管理サービス	ログ管理サービス
	サービス名	セキュリティ監視・診断サービス	InfoCIC
	開発元／販売元	(株)ラック／(株)ラック	(株)インフォセック／(株)インフォセック
	サービス概要	・ユーザ先に設置したファイアウォール、IDS／IPSをインターネット経由でセンターからリアルタイム監視	・ユーザ先に設置したRSA NetWitnessをインターネット経由でセンターからリアルタイム監視
サービス内容	不正アクセス痕跡の定常監視	・ユーザ先に設置したファイアウォール、IDS／IPSを24時間365日リアルタイム監視 ・ラックのエンジニアによる監視ポリシーの運用 ・ラック独自シグネチャ(JSIG)によるSQLインジェクションやボットなど最近の脅威に対応 ・アラート分析により危険度を判定し、必要のある攻撃だけを通知 ・緊急時の連絡とインシデント対策支援	・ユーザ先に設置したRSA NetWitnessを24時間365日リアルタイム監視 ・キーワードによる検知 ・フィルター(基本から始めてカスタマイズ)、ブラックリストによる監視対象の絞り込み ・インフォセック独自の仮想環境(SandBox)上での実行確認
	窃盗された情報の特定	・インシデント対応の中で個別に分析	・記録されたパケットから該当ファイルを抽出
	攻撃元特定に資する情報の抽出	・インシデント対応の中で個別に分析	・RSA NetWitnessの解析機能を利用 ファイル構文分析(File属性／ヘッダ) ファイルの流入経路や流入方法
	その他	・ログの解析は、個別のインシデント対応によって行う ・端末やサーバの監査ログ、ドメインコントローラのログ、プロキシ、ファイアウォール、IDS／IPS等の記録から感染経路追跡、漏えいデータの予測、被害範囲を分析	月次レポート
契約形態等	契約形態	年間契約	年間契約 RSA NetWitnessはレンタルまたは買い取り
	導入コスト	数十万円／月	数十万円／月

【別紙2】ログ・証跡管理に関するサービス

サービスのプロフィール	製品種別	ログ管理サービス	ログ管理サービス
	サービス名	Log Shelter	SecureEagle/SIM
	開発元／販売元	(株)JIEC／(株)JIEC	(株)日立システムズ／(株)日立システム
	サービス概要	・ユーザ先に設置したログ収集サーバにより、お客様のログデータをデータセンター内に構築したLog Shelterサービス環境で、インターネットを経由し、収集・蓄積・分析を行う	・ユーザ先に設置したログ収集装置により、セキュリティログを24時間365日リアルタイムでインターネット経由でセンターがモニタリングし、セキュリティインシデントを迅速に発見、さらに内部統制で求められるエビデンス(証跡)として使える様式のレポートを提供
サービス内容	不正アクセス痕跡の定常監視	・「端末監視ソフトウェア」によって企業内部における不正操作を検知・防止し、ログ統合・証跡管理SaaS「Log Shelter」によって不審操作の監視やインシデント発生時の原因追求を支援するレポートを提供	・ユーザ先に設置したログ収集装置に収集した、業務サーバ、認証サーバ、ファイアウォール、DBMS、IDS/IPS、Webサーバ、入退室等のログを24時間365日リアルタイム監視 ・約300種類以上のログに対応 ・相関分析による侵入経路の特定、事象解析 　入退室ログ＋サーバログイン、連続ログイン失敗＋ログイン成功、認証サーバのユーザIDリスト＋グループウェアのログイン失敗、SQLインジェクション検知＋Webサーバの正常応答 などの相関
	窃盗された情報の特定	・検出したインシデントの個別分析による	・インシデント対応の中で個別に分析
	攻撃元特定に資する情報の抽出	・検出したインシデントの個別分析による	・ファイアウォール、プロキシの監視 　プロキシを経由しない通信、プロキシでの認証失敗、通信先が国外等 ・サーバログ等の監視 　ファイアウォール拒否ログ急増、認証失敗の多発 ・サーバログ、サーバ認証ログの監視 　意図しない再起動、OS異常停止、ログ削除や設定変更、アカウントの追加や削除、パスワードリセット
	その他		
契約形態等	契約形態	導入、運用支援あり	年間契約 RSA NetWitnessはレンタルまたは買い取り 導入支援、運用支援あり
	導入コスト	初期導入費：65万円～ 月額：15万円～ 情報漏えい対策モニタリング・サービス月額：700円／台	初期導入費：52万5000円～ 月額：39万円

#	国	発行機関略称	発行機関名	発行年月	文書番号	文書名	概要・備考	URL	
1	アメリカ	NIST	National Institute of Standards and Technology	2006年9月	SP 800-92	Guide to Computer Security Log Management	コンピュータセキュリティログ管理の基本からログ管理計画の策定法、ログの分析と対応を含む運用までのガイドライン。米国のセキュリティ基準・ガイドラインの多くが、ログ管理に関しては本文書を参照している。	http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf	邦訳(IPA-ISEC) http://www.ipa.go.jp/security/publications/nist/documents/SP800-92-J.pdf
2	アメリカ	NIST	National Institute of Standards and Technology	2006年8月	SP 800-86	Guide to Integrating Forensic Techniques into Incident Response	インシデント対応のガイドであるが、ネットワークフォレンジックに1章が割かれ、各種ネットワーク機器で収集されるログでインシデント対応の際に考慮すべきものに関する記述がある。	http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf	邦訳(IPA-ISEC) http://www.ipa.go.jp/security/publications/nist/documents/SP800-86_J.pdf
3	アメリカ	SANS/GIAC	SANS Institute			A Process for Continuous Improvement Using Log Analysis	セキュリティ教育機関SANSのトレーニング文書。定期的ログ分析レポートにおいて、どのようなイベントをどのように報告すべきかをまとめている。	http://www.giac.org/paper/gsec/29793/process-continuous-improvement-log-analysis/108778	
4	アメリカ	HHS	Department of Health and Human Services	2003年2月		HIPAA (Health Insurance Portability and Accountability Act) Security Rule	ログを取得すべきイベントの種類とログの定期的分析を要求事項として明確にしている。	http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html	
5	アメリカ	DISA	Defense Information System Agency	2006年1月		SECURITY TECHNICAL IMPLEMENTATION GUIDES	OS(Windows、Macintosh、UNIX)、アプリケーション、DB、DNS等サービス毎のセキュリティ技術的実装ガイドで、各文書内にログ実装についての要件を記載。	http://www.disa.mil/	
6	イギリス	NISCC (現CPNI)	Centre for Protection of National Infrastructure	2003年3月		PROTECTIVE MONITORING – INTRODUCTION TO AUDIT AND ACCOUNTING LOG ANALYSIS	ITセキュリティ管理者向けの、ログ分析の基本と悪意あるふるまいに関する技術解説。	http://www.cpni.gov.uk/documents/publications/2003/2003004-tn0303_protective_monitoring.pdf	
7	オーストラリア	DSD	Department of Defense Defence Signals Directorate	2005年		Australian Government Information Security Manual 2012 Controls	政府機関向けセキュリティマニュアル。ACCESS CONTROLの項目にEvent Logging and Auditingとしてログに関する具体的管理策が記載されている。	http://www.dsd.gov.au/infosec/ism/index.htm	
8	オーストラリア	DSD	Department of Defense Defence Signals Directorate	2010年2月		Top 35 Mitigation Strategies	サイバーイントルージョンに対応する35のセキュリティ管理策のリスト。23および24がログの取得と分析に関するもの。	http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm	
9	オーストラリア	DSD	Department of Defense Defence Signals Directorate			Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details	上記リストの具体的解説。	http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm	
10	インド	CERT-In	Indian Computer Emergency Response Team	2008年12月	CISG-2008-01	Guidelines for Auditiong and Logging (Version 2)	管理対象プラットフォーム(Windowsホスト、Linuxホスト、Webサーバ、データベースサーバ)ごとに、取得すべきログの種類を具体的に挙げた文書。	http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=Guideline%20CISG-2008-01	
11	業界標準	PCI SSC	Payment Card Industry Security Standards Council	2010年10月		Payment Card Industry (PCI) Data Security Standard 要件とセキュリティ評価手順 バージョン 2.0	要件10でネットワーク資源およびカード会員情報に対するすべてのアクセスを追跡し、監視することを挙げ、監視すべき項目を具体的に記載している。	https://www.pcisecuritystandards.org/security_standards/documents.php?assocation=PCI%20DSS	