

経済産業省「サイバーセキュリティ経営ガイドライン」

(2015年12月28日発表)

に基づく参考ガイド(JPCERT/CC「高度サイバー攻撃への
対処におけるログ活用と分析方法」)への

NetRAPTOR活用事例紹介

～ネットワークフォレンジック「NetRAPTOR」は証跡記録だけではない！～

トーテックアメニティ株式会社

テクニカルサービス事業部

セキュリティシステム部

経済産業省発表

「サイバーセキュリティ経営ガイドライン」(2015年12月28日発表)

News Release



平成27年12月28日

サイバーセキュリティ経営ガイドラインを策定しました

経済産業省は、独立行政法人情報処理推進機構とともに、「サイバーセキュリティ経営ガイドライン」を策定しました。これに基づき、経営者のリーダーシップの下でサイバーセキュリティ対策が推進されることを期待しています。

1. 策定の背景

様々なビジネスの現場において、ITの利活用は企業の収益性向上に不可欠なものとなっている一方で、企業が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は増加傾向にあり、その手口は巧妙化しています。

そこで、企業戦略として、ITに対する投資やセキュリティに対する投資等をどの程度行うかなど、経営者による判断が必要となっています。

2. サイバーセキュリティ経営ガイドラインの概要

経済産業省では、独立行政法人情報処理推進機構(IPA)とともに、大企業及び中小企業(小規模事業者除く)のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、「サイバーセキュリティ経営ガイドライン」を策定しました。

サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「3原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部(CISO等)に指示すべき「重要10項目」をまとめています。

(本発表資料のお問い合わせ先)
商務情報政策局情報セキュリティ政策室長 瓜生
担当者: 山下、加藤
電話: 03-3501-1511(内線 3964)
03-3501-1253(直通)

サイバーセキュリティ経営ガイドライン

Ver. 1.0

経済産業省

独立行政法人 情報処理推進機構

		大という攻撃フェーズに応じた拡大防止及び緩和を図れる柔軟な対策実施が必要である。	対策の基本』 『継続における内部不正防止ガイドライン』
		● ネットワーク出入りに設置される機器の各種ログが記録・保存され、またこれを内部あるいは外部監視サービスにより定期的にチェックされていない場合、不正な通信の発生を検知することができない。	【ガイド】 JPCERT/CC『高度サイバー攻撃への対処におけるログの活用と分析方法』 IPA『LogScanner』
(4) サイバーセキュリティ対策フレームワーク構築(PCDC)と対策の開示	PCDCサイクルの実施と改善 ISMSの導入やセキュリティ監査の実施によるPCDCサイクルの実施により、現状のセキュリティ対策の改善点を洗い出し、将来の改善計画を立案し実行していくこと。	● 環境や事業の変化に合わせて、対策の点検や改善を継続していない場合、新たな脅威に対処できなくなる恐れがある。	【制度】 NPOC『情報セキュリティマネジメントシステム(ISMS)適合性評価制度』 JIPDEC『サイバーセキュリティマネジメントシステム(CSMS)適合性評価制度』 経済産業省『情報セキュリティ監査制度』 【ツール】 IPA『情報セキュリティ対策ベンチマーク』

JPCERT/CC『高度サイバー攻撃への対処におけるログの活用と分析方法』

引用:経済産業省様 プレス記事サイトより <http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html>

NetRAPTOR 「アラート通知」設定例

～特定ポートへのCONNECTを監視する～

The screenshot shows the NetRAPTOR web interface. At the top, there's a navigation bar with options like '検索' (Search), 'レポート' (Report), '統計' (Statistics), '閲覧ログ' (View Log), 'ダンプデータ' (Dump Data), '設定' (Settings), 'ユーザ管理' (User Management), 'パスワード変更' (Change Password), and 'ログアウト' (Logout). Below this is a search bar with '簡易検索' (Simple Search), '詳細検索' (Detailed Search), and '条件リスト' (Condition List). The main area displays a table of search conditions. One condition is highlighted with a red box and an orange arrow pointing to the detailed view below. The detailed view shows the search condition: '(protocol:http OR protocol:https) AND NOT(url:(":443" ":80")) AND (method:CONNECT)'. Below the detailed view are buttons for '修正' (Edit), '削除' (Delete), and '検索' (Search).

アラート条件	登録者	名前	コメント	対象アナライザ	メール送信先	
警告	初期管理者	443, 80以外のCONNECT	443, 80以外のCONNECT	全アナライザ	登録者	検索 詳細

1 / 1

名前	443, 80以外のCONNECT
検索条件	(protocol:http OR protocol:https) AND NOT(url:(":443" ":80")) AND (method:CONNECT)
コメント	443, 80以外のCONNECT
アラート条件	警告
対象アナライザ	全アナライザ
メール送信先	登録者

修正 削除
検索

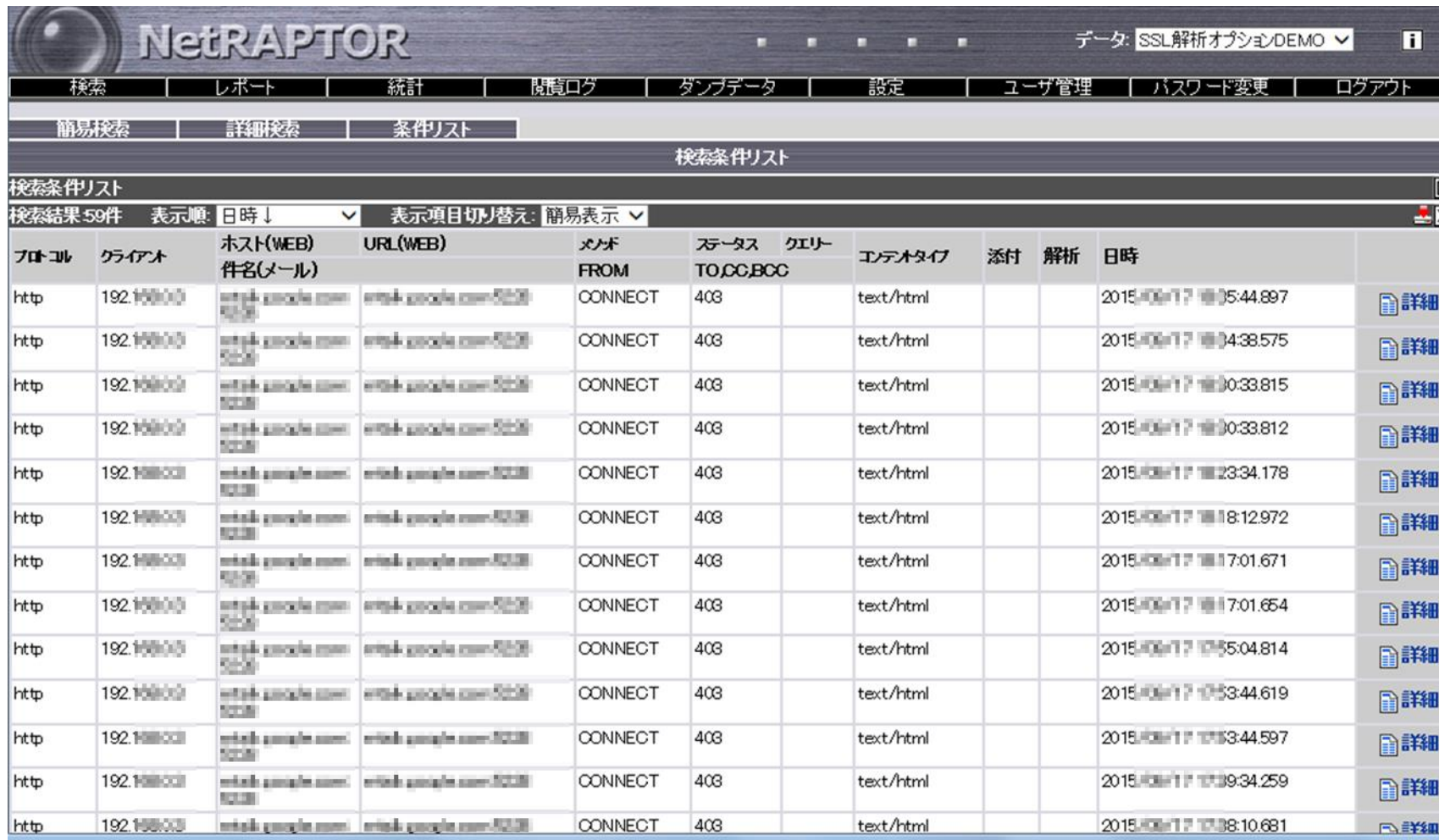
(protocol:http OR protocol:https) AND NOT(url:(":443" ":80")) AND (method:CONNECT)

(http または https プロトコル通信で、ポート443 または 80 以外を利用し、CONNECT方式を使った場合)

NetRAPTORのアラート機能で、該当通信をリアルタイムで管理者にアラート通知が可能

NetRAPTOR 「アラート通知」設定例

～特定ポートへのCONNECT検索結果例 (簡易表示)～



The screenshot displays the NetRAPTOR web interface. At the top, the NetRAPTOR logo is on the left, and the data source is set to 'SSL解析オプションDEMO'. A navigation menu includes '検索', 'レポート', '統計', '閲覧ログ', 'ダンプデータ', '設定', 'ユーザ管理', 'パスワード変更', and 'ログアウト'. Below this, there are tabs for '簡易検索', '詳細検索', and '条件リスト'. The main content area is titled '検索条件リスト' and shows '検索結果 59件'. The results are sorted by '日時' (Date/Time) and displayed in a '簡易表示' (Simple View) format. The table below represents the data shown in the screenshot.

プロトコル	クライアント	ホスト(WEB) 件名(メール)	URL(WEB)	メソッド FROM	ステータス TO,CC,BCC	クエリ	エントタイプ	添付	解析	日時	
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 09:05:44.897	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 09:04:38.575	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 09:00:33.815	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 09:00:33.812	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 08:23:34.178	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 08:18:12.972	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 08:17:01.671	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 08:17:01.654	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 07:55:04.814	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 07:53:44.619	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 07:53:44.597	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 07:39:34.259	詳細
http	192.168.0.0	etask.google.com	etask.google.com/5228	CONNECT	403		text/html			2015/06/17 07:38:10.681	詳細

NetRAPTOR 「アラート通知」設定例

～特定ポートへのCONNECT検索結果例 (詳細表示)～

NetRAPTOR

データ: SSL解析オプションDEMO

検索 レポート 統計 閲覧ログ ダンプデータ 設定 ユーザ管理 パスワード変更 ログアウト

簡易検索 詳細検索 条件リスト

検索条件リスト

検索条件リスト

検索結果 59件 表示順: 日時↓ 表示項目切り替え: 全表示

プロトコル	サーバ	クライアント	MAC アドレス	ホスト(WEB) 件名(メール)	URL(WEB)	メソッド FROM	ステータス TO,CC,BC	クエリ	エンコーディング	添付	解析	日時	
http	192.168.0.100	192.168.0.0	00:e0:4c:ab:10:4a	mtalk.google.com 5230	mtalk.google.com/5230	CONNECT	403		text/html			2015/10/17 11:35:44.897	詳細
http	192.168.0.100	192.168.0.0	00:e0:4c:ab:10:4a	mtalk.google.com 5230	mtalk.google.com/5230	CONNECT	403		text/html			2015/10/17 11:34:38.575	詳細
http	192.168.0.100	192.168.0.0	00:e0:4c:ab:10:4a	mtalk.google.com 5230	mtalk.google.com/5230	CONNECT	403		text/html			2015/10/17 11:30:33.815	詳細
http	192.168.0.100	192.168.0.0	00:e0:4c:ab:10:4a	mtalk.google.com 5230	mtalk.google.com/5230	CONNECT	403		text/html			2015/10/17 11:30:33.812	詳細
http	192.168.0.100	192.168.0.0	00:e0:4c:ab:10:4a	mtalk.google.com 5230	mtalk.google.com/5230	CONNECT	403		text/html			2015/10/17 11:23:34.178	詳細
http	192.168.0.100	192.168.0.0	00:e0:4c:ab:10:4a	mtalk.google.com 5230	mtalk.google.com/5230	CONNECT	403		text/html			2015/10/17 11:18:12.972	詳細
http	192.168.0.100	192.168.0.0	00:e0:4c:ab:10:4a	mtalk.google.com 5230	mtalk.google.com/5230	CONNECT	403		text/html			2015/10/17 11:17:01.671	詳細
http	192.168.0.100	192.168.0.0	00:e0:4c:ab:10:4a	mtalk.google.com 5230	mtalk.google.com/5230	CONNECT	403		text/html			2015/10/17 11:17:01.654	詳細
http	192.168.0.100	192.168.0.0	00:e0:4c:ab:10:4a	mtalk.google.com 5230	mtalk.google.com/5230	CONNECT	403		text/html			2015/10/17 11:15:04.814	詳細
http	192.168.0.100	192.168.0.0	00:e0:4c:ab:10:4a	mtalk.google.com 5230	mtalk.google.com/5230	CONNECT	403		text/html			2015/10/17 11:13:44.619	詳細

「NetRAPTOR」でマルウェア通信の監視

NetRAPTOR(ネットラプター)は、ネットワーク通信のキャプチャ・保存・解析・再現だけでなく、想定外の通信や通信内容を見張ること、管理者に**リアルタイム**アラートメールを送信することが可能です。

設置した瞬間から、マルウェア通信等の不正通信を監視し、**情報漏洩を起こす前に対策**を打つことが可能となります。

お客様を個別に狙った**標的型攻撃**は、メーカーから配布される**対策パタン**では**防衛**できません。標的型攻撃は、**そこに設置したネットワークフォレンジックにしか記録されません。**



AMENITY LIMITED