CySec

ＩＤＦ「ＤＦ人材育成」分科会　資料

ネットワーク・フォレンジック

東京電機大学
八槇　博史

講義概要

- ネットワーク・フォレンジック
  - ネットワーク・フォレンジックの定義
  - デジタル・フォレンジックとの関係
- 標的型攻撃との関係
  - 標的型攻撃の段階
  - 標的型攻撃の検出
- システム群
  - IDS、IPS
  - ログ監視システム
  - SIEM
  - LIFT
- 演習
  - ログ解析
  - パケット解析

ネットワーク・フォレンジックとは

ネットワーク・フォレンジックとは、「セキュリティ上の攻撃や問題を発生させるインシデントの発生源を発見するために、ネットワーク上のイベントをキャプチャ、記録、分析すること」である。

Marcus J. Ranum
セキュリティ・システムの設計や開発の専門家として世界的に有名。プロキシー型ファイアウォールの発明者として、1980年代に最初 の商用ファイアウォールを提供。

各種ネットワーク装置のログ

ファイアーウォール

プロキシーサーバ

IPSのログ

Sysintehral

プロセスとパケットを対応付けたログ

標的型攻撃と対策案

	初期侵入	侵入の拡大	目的の遂行
攻撃法	標的型メール	ぜい弱性をついた攻撃	機密情報の盗み出し
対策案	不正メールの見極め	セキュリティパッチ アクセス制御など	不正送出の検知・防止

対策案：

① パケット系のログ・証跡管理（ネットワーク・フォレンジック）の充実による被害実態の早期把握

② 組織内CSIRT（ computer security incident response team ）の設置と継続的充実による早期対応　など

標的型攻撃対策のための適切なログの管理（その１）

＜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．ログは１年間以上保存する。
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。
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。

内閣官房情報セキュリティセンター：
http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf

標的型攻撃対策のための適切なログの管理（その２）

＜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。
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。
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。

内閣官房情報セキュリティセンター：
http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf

標的型攻撃対策のための適切なログの管理（その３）

＜機器別の対策＞

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。
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。
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。

内閣官房情報セキュリティセンター：
http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf

ネットワーク・フォレンジックの対応フェーズ

	フェーズ１	フェーズ２	フェーズ３	フェーズ４	フェーズ５
対応状況	大多数の企業	→	→	先進的企業	今後
機能		ネットワーク関連ログの収集	各種ログの統合管理	監視情報との統合	管理のインテリジェント化
ツール	なし	パケットログ記録ツール	ログ統合管理ツール	SIEM	LIFT

SIEM:　Security Information and Event Management
LIFT:　Live and Intelligent　Network Forensic Technologies

SIEM製品

セキュリティに関する統合ログ管理と、リアルタイムに高速な分析を行うことにより、異常を検知し異常状況を分かりやすく視覚化するもの

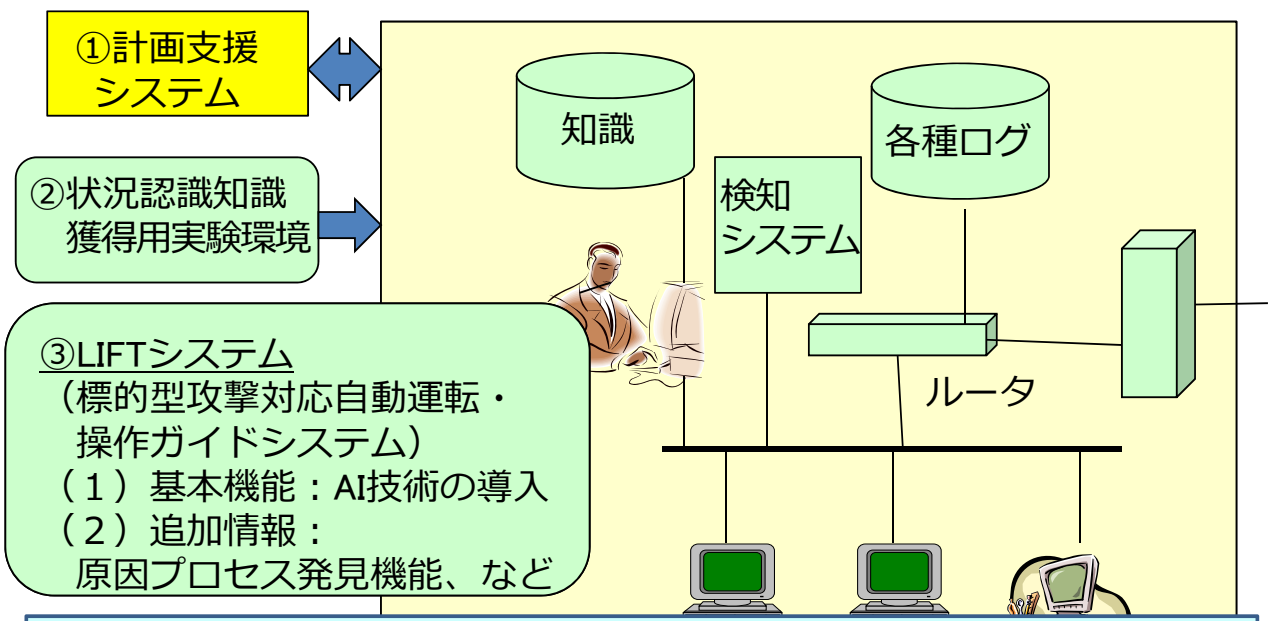
① McAfee Security Information and Event Management（マカフィ）
② IBM Security Qradar　（IBM）
③ SIEMマネジメントサービス　（富士通）ほか

SIEM:　Security Information and Event Management

SIEMの問題点と対策案

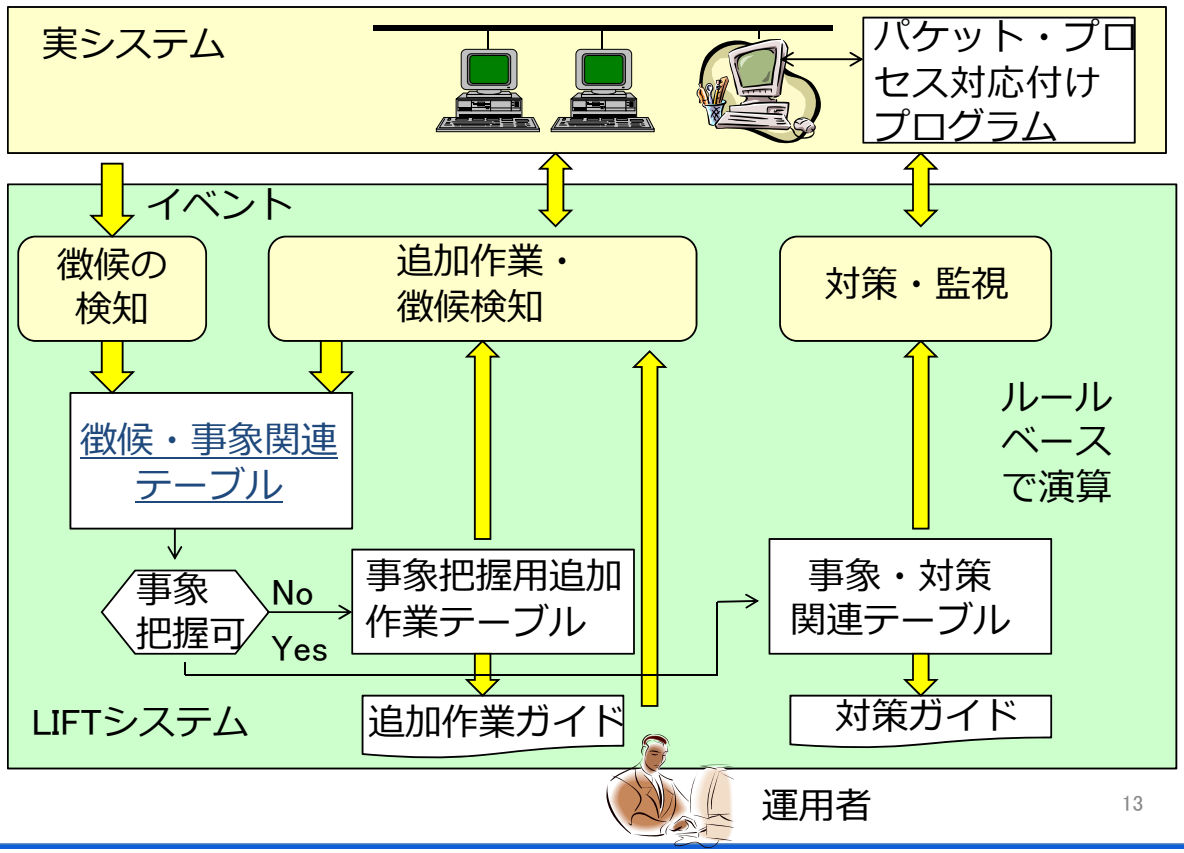
1．対策の総合的判断が過剰に運用者の能力に依存
　（1）判断の自動化
　（2）対応に関する適切なガイド　→ AI技術の活用
2．判断に利用する情報が不十分
　（1）パケットを流した元のアプリケーションの探索方法の確立
　（2）LIVEメモリー情報のトリガーベースの効率的収集
　（3）不当に消されたデータの持つ情報の有効利用
　（4）ゾーンニングなどの能動的行動によって得られる情報の有効利用
　（5）計画支援システムとのリンク
　（6）実証実験システムとのリンク

LIFTプロジェクトの概要



共同開発プロジェクト　（リーダ佐々木、上原先生、高倉先生、八槇先生、柿崎先生、日立他）　期間：2013年9月ー2017年3月（第一期）
現状での主な成果：①方式確立　②原因プロセス発見ソフト製品化

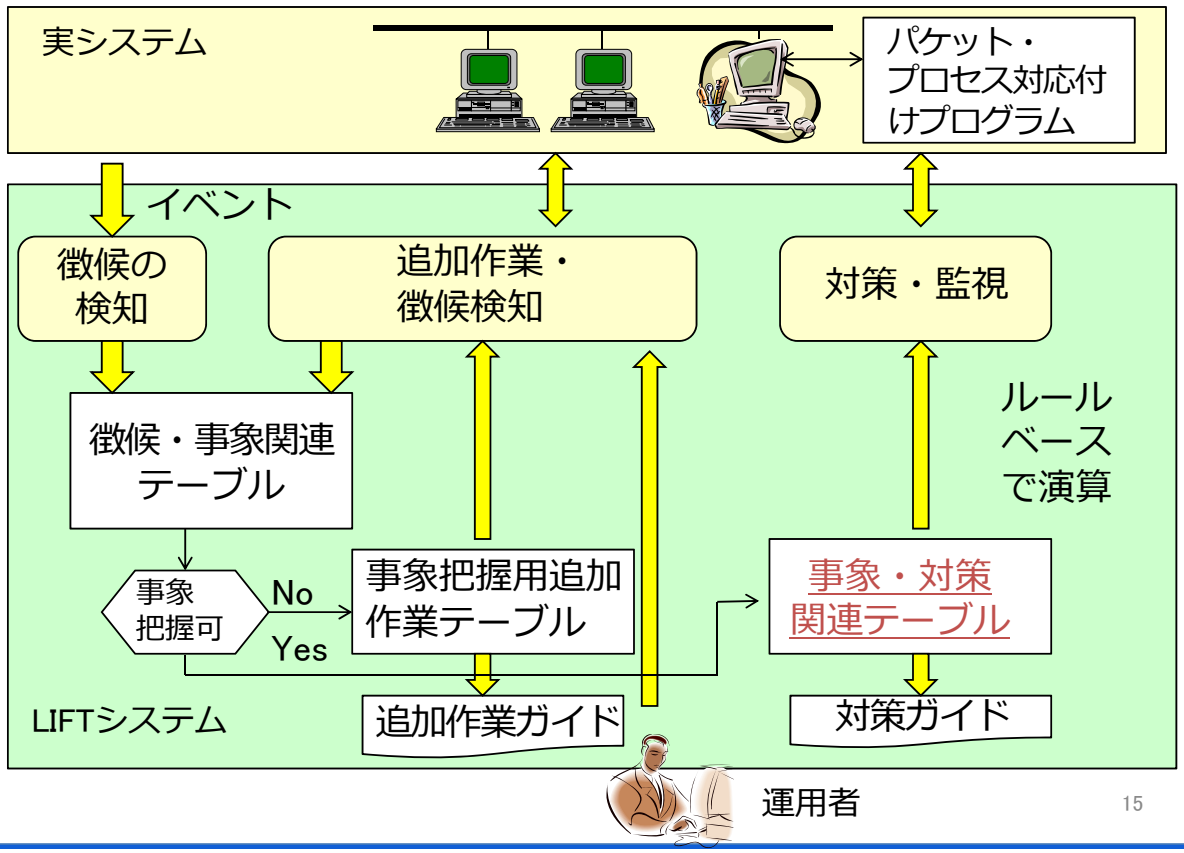
LIFTシステムの運用イメージ



徴候・事象関連テーブルと確信度

	攻撃事象 ＼ 徴候	不自然なプロセスの立ち上がり	プロキシ: プロキシを経由しない通信	プロキシ: 443以外のCONECTメソッドを利用した通信	長時間のセッション	業務に不要なコマンド
基盤構築フェーズ	端末が不正プログラムを起動	0.3				
	C&Cサーバへ接続		0.6	0.6	0.4	
	必要な機能のダウンロード	0.4	0.4		0.3	
	端末の情報入手	0.5			0.2	0.4

LIFTシステムの運用イメージ



ネットワーク・フォレンジックの基本作業

- パケットキャプチャ
  - 通信の解析
  - Wireshark, TCPdump, …
- ログ解析
  - サーバ、ネットワークスイッチ、IDS…
  - 状況分析
- SIEM、LIFT等による自動化

パケットキャプチャ

- ネットワークインタフェースに入力されるデータの記録、分析
  - インシデント対応
  - ネットワークトラブルの原因追及
  - プロトコル解析　etc.

- 「パケット」キャプチャと呼ぶが、実際にはL2のフレームやL4のデータグラムも分析対象
  - 各レイヤに関するプロトコルの知識が不可欠

パケットキャプチャツール

- Wireshark
  - キャプチャしたパケットの解析、フィルタ機能による抽出など
    - 演習で使用方法を説明、実際の解析手順を学ぶ
      - 各種プロトコル：HTTP、HTTPS、SMTP、DNS、DHCP、…
      - フィルタの使用方法
- Tcpdump, Network Miner, Xplico, tcpslice, tcpflow,…

ログ分析

- 各種ログ
  - サーバ、スイッチ、DSなど
  - 演習
    - ログの読み方、設定
    - ログと攻撃内容との関係
      - ブルートフォース攻撃、ポートスキャン etc/
- IDS/IPS
  - アラート

反省事項

- 講義：概略的過ぎた？
  - SIEMの概略までは知っているので、むしろLIFTについてつっこんだところを知りたいという意見
    - CySec初年度生の特質かも．．．
  - 参考文献を充実させてほしい
    - 標準的な文献が確立していない悩み
- 演習：もっとリアルでもよいが、そうするとプロトコルの理解が必須になり時間が不足
  - 時間内で説明できるのはよく知られた事例
  - TCPの3ウェイハンドシェイクを悪用して云々、はわかっている人には簡単だが、知らないと何の話かついていけないという、受講生のちょっとしたレベル差で生まれるギャップ

CySecの観点から

- 多くの問題はデジタル・フォレンジック科目だけの話ではない
- 社会人受講者にとっては易しく、大学院生受講者にとっては難しい傾向
  - 受講者のレベル把握の難しさ
  - 社会人ターゲットという概ねの方針はある
  - 最初の想定よりも一期生のレベルが高い
    - 「これからCSIRT」を想定していたところに「すでにCSIRT」の人が多く来た
- 時間が足りない
  - 入門から話すと学部で半期かかるものを１コマに入れてある

まとめ

- 講義の範囲
  - 定義
  - 標的型攻撃
  - ログ分析、パケット解析
  - 監視システム
- 悩ましいところ
  - 標準的な解釈・教科書の不在
  - どこまで掘り下げるか