情報セキュリティ大学院大学
橋本研究室

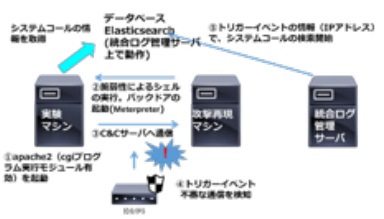
情報セキュリティについて、
アクセス制御を軸に研究を進めています。

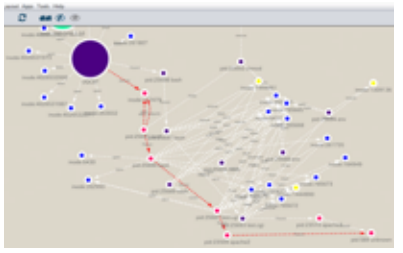
情報セキュリティは情報・通信の安全性を支える基盤であり、アクセス制御はその基礎をなします。橋本研究室は、2015年10月、情報セキュリティ大学院大学情報セキュリティ研究科に新設された研究室で、アクセス制御の理論や実装に関する研究を通じ、より安心・安全・快適で、豊かな情報社会の発展に貢献することを目指します。

主要な研究領域は、オペレーティングシステム・セキュリティとネットワーク・セキュリティで、具体的には、不正侵入検知／防御技術、OSINT/Intelligence Mining、マルウェア解析技術、SELinux、TOMOYO Linux、サイバー攻撃技術、デジタルフォレンジック、Honeypot、ポリシ記述言語等の研究を進めています。

研究事例紹介 I：
知的侵入検知・防御システムの研究

- 研究内容：プロセスの親子関係や実行履歴，ファイルの操作履歴等から一連の活動をリンク付し，事前に悪性活動を定義しておくことで，複雑な攻撃の機械的な判定を可能とする．
  - ❖ 小池拓矢, 大窪巳祐, 辻秀典, 橋本正樹: システム内活動の紐付けによる悪性活動の定義方式に関する研究, 信学技報, Vol.117, No.481, ICSS2017-51, pp.55-60, 2018年2月.

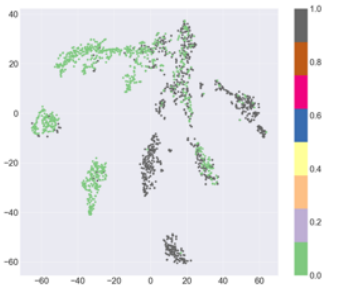


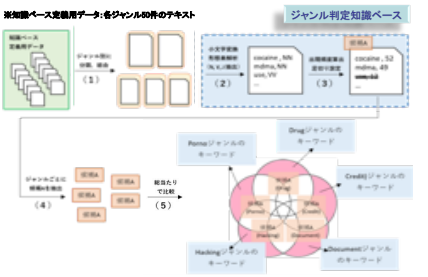


x

研究事例紹介 II：機械学習と推論による
ダークウェブ上情報の検索・分類システム研究

- 研究内容：ダークウェブに存在する多種多様・大量の情報から，機械学習・推論を用いて必要とする情報を識別・分類する．
  - ❖ Masashi Kadoguchi, Shota Hayashi, Masaki Hashimoto, Akira Otsuka: Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning, Proceedings of IEEE ISI 2019), pp. 200-202, Shenzhen, 2019.
  - ❖小林 華枝, 橋本 正樹: ダークウェブ上に蔓延する違法有害情報の自動分類エキスパートシステムの開発, 2020-SPT-36(20), pp.1-6, 2020年2月.

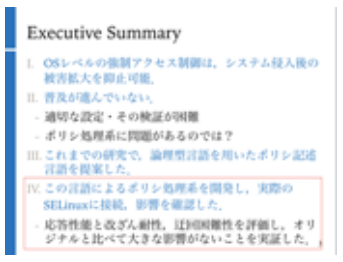




x

研究事例紹介 III：SELinux/TOMOYO Linuxの実用性向上に向けた研究

- 研究内容：強制アクセス制御が普及しない原因は，ポリシ記述・管理の困難さにある．論理型言語を記述と管理に用いることでこの解決を図る．
  - ❖ 橋本正樹, 滝澤峰利, 高山扶美彦, 辻秀典, 田中英彦: 論理型言語による強制アクセス制御の実用的な実装に向けて, 信学技報, vol. 115, no. 334, ICSS2015-44, pp. 55-60, 2015年11月.



x

研究事例紹介 IV：その他の研究例

- HTTPリクエストの調査と偽のUser-Agent値の識別方法の提案
- Processing言語によるセキュアOS/侵入防御効果の可視化手法
- 海事サイバーセキュリティの現状と課題
- 短距離無線通信向け脆弱性検査ツールの初期的検討
- 欺瞞ネットワークの効率的な配置の評価
- 機械学習を用いた偽サイト検知
- TrustZone Technologyを利用したアクセス制御ポリシーの保護手法
- 悪性活動の機能種別に着目した機械学習によるマルウェア検知手法
- メモリ・フォレンジクスツールの評価手法に関する研究
- 機械学習を用いた脅威インテリジェンス抽出手法
- CNNを用いたPE内関数の類似性によるマルウェア検知手法

x

Google 橋本研究室　iisec