様 式 Ｃ－７－１　　該当する研究種目 … 「特別推進研究(COE)」を除く全ての研究種目

平成　　年度科学研究費補助金実績報告書（研究実績報告書）

1. 機 関 番 号　1 4 6 0 3　　2. 研究機関名　奈良先端科学技術大学院大学

3. 研 究 種 目 名　若手研究（B）　　4. 研究期間　平成１６年度 ～ 平成１８年度

5. 課 題 番 号　1 6 7 0 0 0 3 3

6. 研 究 課 題 名　動的命令を用いたソフトウェアプロテクション

7. 研 究 代 表 者

研究者番号	研究代表者名	所属部局名	職名
8 0 3 1 1 7 8 6	ﾌﾘｶﾞﾅ　モンデン　アキト 門田　暁人	情報科学研究科	助教授

8. 研究分担者(所属研究機関名については、研究代表者の所属研究機関と異なる場合のみ記入すること。)

研究者番号	研究分担者名	所属研究機関名・部局名	職名
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		

9. 研究実績の概要(国立情報学研究所でﾃﾞｰﾀﾍﾞｰｽ化するため、600字～800字で記入。図、ｸﾞﾗﾌ等は記載しないこと。)

動的命令を含んだプログラムPをオートマトンにより解釈・実行するシステムを実装した．攻撃者の視点からシステムの安全性を評価し，システムが満たすべき性質について整理するとともに，主に次の２点についてシステム設計の見直しを行った．

（１）動的命令を含むプログラムPから元のプログラムP_0を推測する手がかりとして，(a)分岐オペコード，(b)ダミー命令，(c)オペコード出現頻度の偏り，が存在することが分かった．そこで，(a)(b)の手がかりを隠蔽するために，Pの言語にオートマトンの状態遷移のみを行う命令を追加し，ダミー命令を用いないこととした．これにより，オートマトン上での分岐オペコードとそれ以外のオペコードの区別が不要となった．また，(c)を解決するために，状態遷移関数に次の制約を設けた．全ての $\underline{c_j}$ に対し，$\{\lambda^{i-1}(\underline{c_j}) : 0 \leq i < n\} = \Sigma$ を満たすという制約である．ここで，$\underline{c_j}$ はプログラムP_0の言語に含まれるオペコードであり，nはオートマトンの状態数であり，λ^iは状態iにおける出力関数，Σは全動的命令（オペコード）の集合であり．この意味するところは，任意のオペコードを選び，オートマトンの各状態で動的命令へと変換した場合，得られる動的命令の集合が常に全動的命令の集合と等しくなるということである．

（２）オペランドを隠蔽するために，1対多の写像を用いた．例えば，オペコードが２バイトのオペランドop1，op2を取る場合，オペランドをb1，b2，b3，b4，b5の５バイトに拡張する．ただし，b3，b4，b5は一様分布0,…,255からランダムに選ばれる値であり，また，b1‖b2 = {op1‖op2} XOR {R_i(b3)‖R_i(b4)} XOR {R_i(b5)‖R_i(b5)}とする．ここで，R_iはオートマトンの各状態iに対応付けられる１バイト幅の全単射である．

※　成果の公表を見合わせる必要がある場合は、その理由及び差し控え期間等を記入した調書(A4 判縦長横書 1 枚)を添付すること。

10. キーワード

(1) ソフトウェアの難読化　(2) ソフトウェアクラック　(3) 耐タンパーソフトウェア
(4) 情報隠蔽　(5) 有限状態機械　(6)
(7)　(8)

（裏面に続く）

11.研究発表(平成１７年度の研究成果)

〔雑誌論文〕　計（ ６ ）件

著　　者　　名	論　　文　　標　　題			
Yuichiro Kanzaki	A software protection method based on instruction camouflage			
雑　　誌　　名		巻・号	発 行 年	ページ
Electronics and Communications in Japan, Part 3		89. 1	2006	47-59

著　　者　　名	論　　文　　標　　題			
Haruaki Tamada	Java birthmarks - detecting the software theft			
雑　　誌　　名		巻・号	発 行 年	ページ
IEICE Transactions on Information and Systems		E88-D. 9	2005	2148-2158

著　　者　　名	論　　文　　標　　題			
Hiroki Yamauchi	Software obfuscation from Crackers' Viewpoint			
雑　　誌　　名		巻・号	発 行 年	ページ
Proceedings of IASTED International Conference on Advances in Computer Science and Technology			2006	286-291

著　　者　　名	論　　文　　標　　題			
門田 暁人	ソフトウェアプロテクションの技術動向(前編) - ソフトウェア単体での耐タンパー化技術			
雑　　誌　　名		巻・号	発 行 年	ページ
情報処理		46. 4	2005	431-437

著　　者　　名	論　　文　　標　　題			
門田 暁人	ソフトウェアプロテクションの技術動向(後編) - ハードウェアによるソフトウェア耐タンパー化技術			
雑　　誌　　名		巻・号	発 行 年	ページ
情報処理		46. 5	2005	558-563

著　　者　　名	論　　文　　標　　題			
山内 寛己	攻撃タスクを考慮した難読化による暗号プログラムの保護			
雑　　誌　　名		巻・号	発 行 年	ページ
電子情報通信学会技術報告		SS2005-60	2005	31-36

〔図　書〕　計（ ０ ）件

著　　者　　名	出　　版　　社		
書　　名		発 行 年	総ページ数

12. 研究成果による工業所有権の出願・取得状況

計（ ０ ）件

工業所有権の名称	発明者	権利者	工業所有権の種類、番号	出願年月日	取得年月日