様 式 Ｃ－７－１

平成１８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 １４６０３　　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 １６７００３３

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
８０３１１７８６	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。)

前年度に行ったシステム設計の見直しに基づいて，動的命令を含むプログラムPを作成するシステムを試作・評価を行い，さらなる安全性の向上について検討した．

試作システムを用いてPを作成し，Pに含まれるオペコードの値の分布に基づいてPの安全性を評価した結果，システム設計の見直しによって標準偏差が38.83から13.47に改善し，ガウス分布を仮定した場合の（理想的な）標準偏差である12.7に非常に近い値を取ることが確認できた．このことから，攻撃の手がかりが大きく減じたといえる．

ただし，次の2点が依然として課題として残っている．(1)Pの各行に存在する動的命令（オペコード）は，実行時にそれぞれ一意に解釈されるため，Pを暗号文とみなして暗号解読を行うことが可能であり，元のプログラムP0が推測される可能性がある．(2) Pは，一般に，ライブラリ関数と呼ばれる外部のプログラムを呼び出す場合があり，この呼び出しの存在が攻撃者に手がかりを与える．

そこで，(1)(2)をそれぞれ解決するための要素技術について検討した．まず，(1)を解決するために，命令列の畳込みという新しい概念を導入し，類似する命令列を一つの命令列にまとめ，それら命令列間の差分を，自己書き換えにより必要な命令（オペコード，及び，オペランド）に置き換える方法を提案した．これにより，Pの各命令は必ずしも一意な解釈を持たなくなり，単純な暗号解読に対する耐性を高めることができた．

また，(2)を解決するために，Pに含まれるライブラリ関数の名前を暗号化し，それらをPの実行時に復号し，リフレクションや動的リンクの機構を用いて関数を呼び出す方法を提案した．これにより，Pに含まれるライブラリ関数の名前を隠すことが可能となった．

※ 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) 命令列の畳込み　(6) 動的リンク
(7)　(8)

（裏面に続く）

11.研究発表(平成１８年度の研究成果)

〔雑誌論文〕　計（６）件

著者名	論文標題
西岡 隆司	類似した命令列の畳込みによるプログラムの耐タンパ性の向上

雑誌名	巻・号	発行年	ページ
情報処理学会研究報告	2007-SE-155-22	2007	167-174

著者名	論文標題
神崎 雄一郎	高級言語レベルでの偽装内容の指定が可能なプログラムのカムフラージュ

雑誌名	巻・号	発行年	ページ
2007年暗号と情報セキュリティシンポジウム(SCIS2007)	4D1-3	2007	(CD-ROM)

著者名	論文標題
玉田 春昭	C言語におけるライブラリ呼び出し隠蔽のための名前難読化手法

雑誌名	巻・号	発行年	ページ
2007年暗号と情報セキュリティシンポジウム(SCIS2007)	4D1-2	2007	(CD-ROM)

著者名	論文標題
玉田 春昭	Javaクラスファイル難読化ツールDonQuixote

雑誌名	巻・号	発行年	ページ
ソフトウェア工学の基礎XIII		2006	113-118

著者名	論文標題
岡本 圭司	API呼び出しを用いた動的バースマーク

雑誌名	巻・号	発行年	ページ
電子情報通信学会論文誌D	Vol.J89-D, No.8	2006	1751-1763

著者名	論文標題
Y. Kamei	Empirical Evaluation of SVM-based Software Reliability Model

雑誌名	巻・号	発行年	ページ
Proc. of 5th International Symposium on Empirical Software Engineering (ISESE2006)	Vol.2	2006	39-41

〔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