平成３０年度情報セキュリティに関する
懸　賞　論　文　の　募　集

公益財団法人 防衛基盤整備協会では、情報セキュリティに関する意識の向上を目的に、情報セキュリティに関する懸賞論文を広く募集しています。	
論　文 テーマ	１ 指定テーマ ⑴ 情報セキュリティにおける経営者の責任 ⑵ 実践的情報セキュリティフレームワークの構築に向けた要員確保と人材育成 ⑶ サプライチェーンにおける情報セキュリティの確保 ⑷ 中小防衛関連企業におけるＮＩＳＴ ＳＰ８００-１７１適用のための課題 ⑸ 学校教育で行うべき情報セキュリティ教育 ⑹ ＡＩ技術が情報セキュリティにもたらす影響と対策 ⑺ 情報セキュリティの面から見た仮想通貨に関する諸問題に対する提言 ⑻ スマートフォンの情報セキュリティ対策 ２ 自由テーマ（キーワードを使用：別紙第２参照）
募集期間	５月７日（月）～９月２１日（金）
表　彰	１　受賞作品：４件以内 ２　副　　賞：総額８０万円
表彰状贈呈式及び祝賀会	１ 時　期：平成３１年１月２２日(火)予定(予備１７日(木)) ２ 招待者：防衛事務次官、防衛審議官、防衛装備庁長官 大臣官房長、防衛省各局長　等
受賞作品の紹介等	１ 協会ホームページへの掲載 ２ セキュリティ産業新聞への掲載依頼 ３ 受賞作品の小冊子を作成・配付（配付先：各省庁、外郭団体（独立行政法人情報処理推進機構、日本ｾｷｭﾘﾃｨ･ﾏﾈｼﾞﾒﾝﾄ学会等)、各都道府県公立図書館、防衛調達関連企業　等） ４ 受賞者の中から、平成３１年２月開催予定の情報セキュリティ講演会（例年約１７０名の参加）での講演を予定
詳しくは、別紙の「平成３０年度情報セキュリティに関する懸賞論文募集要項」をご覧ください。	
問い合せ先	〒160-0003 東京都新宿区四谷本塩町 15 番 9 号 ラボ東京ビル 7 階 公益財団法人　防衛基盤整備協会 防衛基盤研究センター 業務部 企画課　担当：五十嵐 TEL 03-3358-8754　　FAX 03-3358-8735 E-mail:koueki@bsk-z.or.jp　URL https://ssl.bsk-z.or.jp

別　紙

平成３０年度情報セキュリティに関する懸賞論文募集要項

1　目的

公益財団法人　防衛基盤整備協会は、公益目的事業として、広く国民の皆様に対し、情報セキュリティに関する正しい知識を広め、理解を深めていただくために各種の事業を行っています。

この中で情報セキュリティに関する懸賞論文を募集・表彰する本事業は、多くの方から論文を応募していただくことを通して、情報セキュリティ意識を高めるとともに、情報セキュリティ技術の発展を促し、多くの皆様に情報セキュリティに関する理解を深めていただくことを目的にしています。

2　情報化社会のセキュリティの現状

情報通信技術は社会経済や安全保障の基盤であるばかりでなく、個人の生活レベルにおいてもあらゆるものが依存しています。しかし、コンピューターやネットワークの脆弱性を突いて攻撃を仕掛けてくるサイバー攻撃は情報化社会の大きな脅威となっています。

サイバー攻撃の脅威は、企業や組織の規模の大小や業種・業界に関係なく、また、企業や組織に重要な情報がないとしても、取引先への攻撃の踏み台にするために侵入される可能性があります。サイバー攻撃の手法は日々、巧妙化、複雑化し、セキュリティリスクはかつてなく高まっています。

便利さだけでなくセキュリティリスクも伴う情報化社会・インターネット社会のセキュリティ対策等をどのように進めるべきか、社会をどのように啓発していけばよいか等大きな課題となっています。

3　論文テーマ

今年度の懸賞論文のテーマは、指定テーマ又は自由テーマ（キーワードを使用）とします。それぞれのテーマについて、皆様が日ごろ重要だと考えている視点からの取り組みの事例や提案、考察又は創造性に富んだアイデア・提言を論文にまとめて下さい。

なお、読み手がそれぞれのテーマについて理解を深められるよう、具体的かつ分かり易い内容の論文を期待しています。

（１）指定テーマ

次の中からテーマを選択して、論文を作成して下さい。

①情報セキュリティにおける経営者の責任

②実践的情報セキュリティフレームワークの構築に向けた要員確保と人材育成

③サプライチェーンにおける情報セキュリティの確保

④中小防衛関連企業における NIST SP800-171 適用のための課題

⑤学校教育で行うべき情報セキュリティ教育

⑥AI 技術が情報セキュリティにもたらす影響と対策

⑦情報セキュリティの面から見た仮想通貨に関する諸問題に対する提言

⑧スマートフォンの情報セキュリティ対策

（２）自由テーマ

グルーピング内のキーワードを使用したテーマを応募者自身が選択して、論文を作成して下さい。

【情報セキュリティ体制】

①セキュリティマネジメント

②ネットワーク監視

③セキュリティ・インシデント

④セキュリティ設計・実装

⑤セキュリティポリシー

⑥暗号

⑦パスワード

⑧クラウドとセキュリティ

⑨FedRAMP（Federal Risk and Authorization Management Pratform）

【情報セキュリティをめぐる近年の動向】

⑩ＩｏＴ

⑪ＡＩ

⑫スマートフォン

⑬NIST SP８００－１７１

【サイバー攻撃】

⑭標的型攻撃

⑮マルウェア（ウィルス）

【認証制度】

⑯ＩＳＭＳ

⑰プライバシーマーク

【法律】

⑱我が国のサイバー法制

⑲（ＥＵ）ネットワークおよび情報システムのセキュリティに関する指令（NIS 指令）

⑳（ＥＵ）一般データ保護規則（GDPR（General Data Protection Regulation））

㉑（米国）２０１５年サイバーセキュリティ法

【情報セキュリティの人的側面】

㉒セキュリティ教育

㉓サイバーセキュリティ人材育成

㉔インターネットモラル

㉕インサイダー脅威

【情報の性質に着目した情報保護の態様】

㉖保護すべき情報（CUI：Controlled Unclassified Information）

㉗重要技術情報

㉘企業秘密（営業秘密）

４　応募規定等

（１）応募作品は応募者本人によるもので、日本語の論文とし、３，０００～８，０００字を基準とします。（ただし、表紙、目次、添付資料、データ・図表、参考資料、ページ番号は文字数に含みません。）図表や写真はカラーでも構いませんが、印刷の関係上、白黒となります。

（２）表彰の対象は、募集要項により応募のあった懸賞論文です。

ただし、論文は未発表、未提出のものであり、既発表論文、既提出論文の応募はできません。表彰状贈呈式当日まで発表予定のないものとします。

発表済みの論文に著しく似ている論文は、審査対象外となることがあります。

（３）応募期間は、平成３０年5月7日（月）～9月２１日（金）です。（当日の消印有効）

（４）図表等を他の文献から転用した場合は、その出典元を明記してください。

引用・転載の明記がなく引用・転載された論文は、審査対象外となる場合があります。

（５）応募作品の様式等

ア　論文はワープロソフト（ＭＳ－Ｗｏｒｄ（バージョン：Ｗｏｒｄ２０１３以降））で作成してください。手書き原稿は、審査対象外となります。

イ　Ａ４版　横書き　３４行×３６字を標準とし、ＭＳ明朝１２ポイント。余白は、上３５mm、下 30mm、左 30mm、右 30mm に設定して下さい。

ウ　論文提出方法は、メール、ＦＡＸ又は郵送とします。

エ　応募原稿の表紙に、論文のテーマを記載して下さい。なお、氏名、連絡先、連絡手段を必ず記載して下さい。

オ　論文本文には必ずページ番号を付して下さい。

（6）論文の書き方の基本的事項（参考）

ア　書き方のルール

（ア）一つの論文の中では、漢字にするか仮名表示にするか、送り仮名の表記法（「行う」か「行なう」かなど）を統一してください。外来語の表記法も同じ（サーバとするかサーバーとするか、など）です。

（イ）主語のない文章を書かないでください。主語がない文章は、曖昧さを内包します。

（ウ）1 文は 100 字以内を目安にしてください。また、長いパラグラフも読みにくいので、 1～3 文程度で改行するよう配慮してください。

イ　参考文献を示す

（ア）先行研究をしっかり整理し、今どんな課題が存在しているのかを確かめることが大切です。必ず、論文作成にあたって参考にした本や雑誌などは明記してください。その際には、<1> 著者または編者、<2> 訳者、<3> 書名、<4> 出版社名、<5>出版年を明記して下さい。統計・資料を利用したり、表や図を転用したりする時にも、出所を明示することが必要です。また、何らかのホームページを参照したり、そこから引用したりした場合には、 URL とページを開いた年月日（最終検索日）を明記して下さい。

（イ）書籍の引用例

(本文)

ローレンス・レッシグは、実社会と同様、インターネット社会(サイバー空間)における統制の要素として、「法」「市場」「規範」「アーキテクチャ(＝コード)」があることを明らかにした上で、アーキテクチャが支配し、またその影響力が増大することにより「自由」が喪失されることを防止する観点から、「法」の役割に期待している[1]。

(脚注における引用の表示)

[1] レッシグ, ローレンス・山形浩生(訳)・柏木亮二(訳)[2001]『CODE―インターネットの違法・合法・プライバシー』翔泳社

（ウ）ウェブの引用例

(本文)

我が国においては、インターネットの本格的な普及は 90 年代後半に始まり、2012 年末現在において、普及率は人口比において 79.5 パーセントにまで達することになった[1]。

(脚注における引用の表示)

[1] 総務省[2013]「平成 24 年通信利用動向調査」<http://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html> (2014 年 1 月 13 日確認)"

ウ　脚注のつけ方

脚注は、本文を補足説明しておく必要があると思われる場合や、引用した文献・資料あるいは本文の記述に際して参照したものを明らかにする場合につけます。本文の関連部分の末尾の右上に番号をつけます。Ｗｏｒｄの「脚注の挿入」を使用することを推奨します。

エ　図や表を挿入する場合

論文中に図や表を挿入することは、客観的なデータをもとに議論を進めたり、内容を根拠づけたりする上で効果的です。図や表を挿入する場合には、図または表の通し番号、タイトル、出典を明記して下さい。

5　表彰の内容

受賞者（個人又はグループ）には、次の賞状等を贈呈

（１）賞状：4 件以内

（２）副賞：総額８０万円

6　表彰状贈呈式及び祝賀会

（１）時期及び場所

平成３１年1月２２日（火）予定（予備１７日（木））　ホテルグランドヒル市ヶ谷

（２）招待者

防衛事務次官、防衛審議官、防衛装備庁長官、大臣官房長、防衛省各局長　等

細部は別途計画します。

7　選考等

（１）論文は部外及び部内の専門家で構成する「情報セキュリティ論文選考等委員会」において公平、適正に審査及び選考を行い、受賞者は、平成３０年１１月下旬頃、本人に通知します。

（２）受賞者は表彰状贈呈式に出席して頂きます。

（３）委員会委員から、論文の内容についてお尋ねする場合がありますので、あらかじめご了承下さい。

8　作品の取扱い

（１）応募された作品は返却いたしません。

（２）受賞作品の著作権は当協会に帰属するものとします。受賞作品の無断転載・複製は禁じます。

9　受賞作品の紹介等

（１）受賞作品のホームページへの掲載

受賞作品は、表彰状贈呈式終了後、当協会のホームページに掲載します。

（２）受賞作品のセキュリティ産業新聞への掲載を依頼

受賞作品は、表彰状贈呈式終了後、掲載される予定です。

（３）受賞作品を掲載した小冊子の作成及び配布

受賞作品を掲載した小冊子を作成し、各省庁、外郭団体（独立行政法人情報処理推進機構、日本セキュリティ･マネジメント学会等）、各都道府県公立図書館、防衛調達関連企業等に配付するとともに、当協会主催の情報セキュリティ講演会等の参加者に配布します。

（４）受賞者の中から、平成３１年２月開催予定の情報セキュリティ講演会での講演を予定します。

10　その他

（１）表彰状贈呈式参加にあたり、肖像権は主催者に帰属します。

（２）受賞者の所属組織名（企業名、学校名など）及び氏名は公表させていただきます。

（３）応募申込の際に入手した個人情報は、情報セキュリティの表彰事業に関する目的以外には使用致しません。付紙「個人情報に関する同意書」に同意の上、ご応募下さい。

11　過去の受賞作品

（１）多様化するＩＴ現場におけるＯＯＤＡによるインシデント対応の提案(29 年度)

（２）ＩｏＴセキュリティ通信を支える量子暗号無線通信の実現に向けて(29 年度)

（３）中小企業における情報セキュリティ３つの『ない』の解決策に関する一考察(29 年度)

（４）諸外国におけるサイバーセキュリティ能力拡張の動向(29 年度)

（５）情報セキュリティ教育におけるケーススタディの有効性に関する考察(27 年度)

（６）サイバー人材不足の解決策に関する一考察(27 年度)

（７）ＩｏＴデータの管理上の課題と対応策の考え方(27 年度)

（８）子どものインターネットモラル意識を向上させるための方法(26 年度)

（９）セキュリティ・インシデントによるデータ消失の場合の損害の填補（26 年度）

(10) 標的型攻撃に関する分析と対策計画時における合意形成支援システム(26 年度)

(11) デジタルネイティブから見たインターネットモラル(26 年度)

公益財団法人防衛基盤整備協会ホームページに 20 年度から 29 年度までの受賞作品を掲載しています。

ＵＲＬ　https://ssl.bsk-z.or.jp

12　応募及び問い合わせ先

公益財団法人　防衛基盤整備協会　防衛基盤研究センター

業務部企画課　担当：五十嵐

℡：０３－３３５８－８７５４　fax：０３－３３５８－８７３５

E-mail:koueki@bsk-z.or.jp　　https://ssl.bsk-z.or.jp

〒160-0003　東京都新宿区四谷本塩町１５番９号　ラボ東京ビル７階

付　紙

個人情報に関する同意書

公益財団法人防衛基盤整備協会（以下「当協会」という。）は、業務の遂行上必要なため貴方様に関する個人情報をご提供いただいております。ご提供いただいた個人情報の取扱いについては下記のとおりとなっております。内容をご確認の上、ご応募下さい。また、内容にご同意いただけない場合やご質問がある場合は、担当者または最下部の＜個人情報苦情及び相談窓口＞までお申し出ください。

【個人情報保護管理者】

公益財団法人防衛基盤整備協会　専務理事

【利用目的)

情報セキュリティの表彰事業に係る業務のために利用します。

【第三者への提供】

法令等に基づく場合を除いて、当個人情報を本人の同意を得ずに第三者へ提供することはありません。

【委託】

当個人情報の取扱いの委託を行う予定はありません。

【個人情報提供の任意性】

貴方様が当協会に対して個人情報を提供することは任意です。ただし、個人情報を提供されない場合には、情報セキュリティの表彰事業にかかる事務処理等について支障が生じる恐れがあります。

【個人情報の開示等の求めについて】

当協会では、当個人情報に関する開示等の求めを受け付けております。その手続きについては、個人情報苦情及び相談窓口へご連絡ください。ただし、法令等に基づく場合は、開示等できない場合がります。あらかじめご了承ください。

【提出書類について】

ご提供いただく書類は、業務の終了後もご返却致しません。同書類は当協会にて適切に破棄致します。

＜個人情報苦情及びご相談窓口＞

公益財団法人　防衛基盤整備協会

個人情報保護管理者　専務理事

苦情及び相談窓口責任者　総務部長

TEL：03-3358-8720／FAX：03-3358-8752／メール：jim@bsk-z.or.jp

上記に同意の上、応募申込を行うにあたり個人情報を提供します。
（同意される場合は、☑を入れてください。）

同意　□