アクセス制御機能に関する技術の研究開発の状況

１　国で実施しているもの

総務省又は経済産業省が取り組むアクセス制御機能の研究開発に関してとりまとめたものであり、具体的には、独立行政法人自ら又は委託による研究、国からの委託又は補助による研究である。

実施テーマは以下の３件であり、その研究開発の概要は、別添１のとおりである。

サイバーセキュリティ技術の研究開発
Ｗｅｂ媒介型攻撃対策技術の実用化に向けた研究開発
欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発

２　民間企業等で研究を実施したもの

(1)　公募

警察庁、総務省及び経済産業省が平成30年12月７日から平成31年１月25日までの間にアクセス制御機能に関する技術の研究開発状況の募集を行ったが、その結果、提案はなかった。

(2)　調査

警察庁が平成30年９月に実施したアンケート調査に対し、アクセス制御技術に関する研究開発を実施しているとして回答のあった大学及び企業は次のとおりである。

ア　大学（４大学）
京都産業大学（２件）
佐賀大学（２件）

イ　企業（１社）
住友電気工業株式会社

また、それぞれの研究開発の概要は別添２のとおりである。

なお、別添２の内容は、アンケート調査の回答内容を原則としてそのまま掲載している。

アンケート調査は、以下の条件に該当する大学及び企業の中から、調査対象として無作為抽出した大学334校、企業1,286社の計1,620団体を対象に実施した。

・大学
国公立・私立大学のうち、理工系学部又はこれに準ずるものを設置するもの

・企業
市販のデータベース（四季報）に掲載された企業であって、業種分類が「情報・通信」「サービス」「電気機器」「金融」であるもの

（別添１）

対象技術　インシデント分析技術
テーマ名　サイバーセキュリティ技術の研究開発
開発年度　平成18年度～
実施主体　国立研究開発法人情報通信研究機構 **法人番号**　7012405000492
背景、目的 サイバー攻撃の急増と被害の深刻化によりサイバーセキュリティ技術の高度化が不可欠となっていることから、ネットワークを介したサイバー攻撃やマルウェア等の活動を大局的に把握・対応するための各種観測技術、分析技術、可視化等の研究開発を行う。
研究開発状況（概要） これまでに研究開発・整備したサイバー攻撃観測機構や、マルウェアの収集・分析機構に関して、世界規模の観測網確立に向けた観測規模の更なる拡充、より高度な観測・分析機構の開発等を行った。観測・分析結果については、Webサイト等で広く公開するとともに、アラートシステム等の外部への技術移転を行った。また、地方自治体へのアラート提供を拡大する等、研究開発成果の社会展開を推進した。
詳細の入手方法（関連部署名及びその連絡先） 国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所　サイバーセキュリティ研究室　042-327-6225
将来の方向性 上記の研究開発を通じて、将来のネットワーク自身及びネットワーク上を流通する情報の安全性・信頼性の確保と、利用者にとって安全・安心な情報通信基盤の実現を目指す。

対象技術　インシデント分析技術

テーマ名　Web媒介型攻撃対策技術の実用化に向けた研究開発

開発年度　平成28年度～平成32年度

実施主体　株式会社KDDI総合研究所、国立大学法人横浜国立大学他（国立研究開発法人情報通信研究機構が実施する委託研究の委託先）

法人番号　5030001055903（KDDI総合研究所）、6020005004971（横浜国立大学）

背景、目的

Webを媒体としたサイバー攻撃は拡大の一途を辿っており、情報処理推進機構（IPA）が公表している「情報セキュリティ 10大脅威2015」においても、Web系の脅威が約半数を占め、国民の関心は高い。平成27年6月に公表された日本年金機構からの年金情報流出においては、不正なWebサイトへの誘導も行われたと報道されており、Web系の脅威とその対策は依然、重要課題である。

また、従来からあるWebの改ざんや「ドライブ・バイ・ダウンロード攻撃」に加え、標的型攻撃にWebサーバを利用する「水飲み場攻撃（watering hole attack）」や、オンラインバンキングユーザを狙ってWebブラウザ経由で情報を窃取する「バンキングマルウェア」、検索エンジン経由で不正なWebサイトに誘導する「SEO（Search Engine Optimization）ポイゾニング」など、攻撃手法が多様化・複雑化してきている。さらに、攻撃対象がWindows OSのみならず、Mac OSやAndroid等のモバイル端末、IoT機器（linux組込み系機器）にまで広がってきており、重大な社会問題となっている。

そこで、これまで機構が委託研究として取り組んできた「ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発」（平成24年度～平成27年度）を実用化に向けてさらに発展させ、観測対象をWindows OSのみならず、Mac OSやモバイル端末、IoT機器等に拡大するとともに、Webを媒体とした新たなサイバー攻撃への抜本的な対策に資する観測・分析・対策技術を確立する。

研究開発状況（概要）

平成28年度から以下の研究開発を開始。平成30年度に行った中間評価の結果、平成32年度までの延長を決定。

（１）新型ブラウザセンサの研究開発
（２）新型観測機構の研究開発
（３）新型攻撃情報分析基盤の研究開発
（４）Web媒介型攻撃対策技術大規模・長期実証実験

詳細の入手方法（関連部署名及びその連絡先）

国立研究開発法人情報通信研究機構 イノベーション推進部門 委託研究推進室
（http://www.nict.go.jp/collabo/commission/itaku_kadai_h30.html）
（http://www.nict.go.jp/collabo/commission/k_190.html）
電話 042－327－6011

将来の方向性

上記セキュリティ対策技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

対象技術　侵入検知・防御技術、ぜい弱性対策技術

テーマ名　欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発

開発年度　平成30年度～平成33年度

実施主体　東日本電信電話株式会社、学校法人慶應義塾他（国立研究開発法人情報通信研究機構が実施する委託研究の委託先）

法人番号　8011101028104(東日本電信電話株式会社)、4010405001654（学校法人慶應義塾）他

背景、目的

本研究開発は、欧州との連携により研究開発の促進が期待できる領域について、欧州委員会（EC: European Commission）と連携して共同で実施するプログラム。

ハイパーコネクテッド社会の実現に向けて、実践的なサイバーセキュリティ技術の研究開発は不可欠である。そのため、セキュリティ、IoT、クラウド及びビッグデータを組み合わせた先端技術の研究開発及び実証を通じ、世界規模で有効かつ実効性のあるサイバーセキュリティ基盤技術の構築を目指す。

研究開発状況（概要）

平成30年度から研究開発を開始。

具体的には、「新たな脅威への機敏な対応」、「脆弱性自動検出/自動修復」、「セキュリティツールのオープンソース化」、「IoTセキュリティ」、「クラウドセキュリティ」、「データセキュリティ」、「プライバシー保護」、「データ匿名化」、「IoT／クラウドに関するブロックチェーン」、「重要インフラ保護」、「クロスボーダ・アプリケーション」に関わる研究開発及び実証を行う。

詳細の入手方法（関連部署名及びその連絡先）

国立研究開発法人情報通信研究機構 イノベーション推進部門 委託研究推進室
（http://www.nict.go.jp/collabo/commission/itaku_kadai_h30.html）
（http://www.nict.go.jp/collabo/commission/k_195.html）
電話 042－327－6011

将来の方向性

国際標準化を睨んだ研究開発力の強化や国際実証環境の構築を軸とした共同研究開発に取り組むことにより、情報通信基盤の共通化を通じた豊かな社会への貢献に資する。

（別添２）

ア　大学

企業・大学名	学校法人京都産業大学
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： SHIELD PBI指静脈認証サービス 開発元(メーカー名等)： 株式会社日立システムズ 開発国： 日本 価格： 発売時期： 平成28年2月18日頃～ 出荷数：	下記ページを参照ください。http://www.hitachi-systems.com/solution/s0307/pbi/index.html 該当商品の全機能に関わったわけではなく、認証連携部分について日立システムズ社と共同研究を実施し、その成果が含まれているというものです。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	○
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	学校法人京都産業大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	
ホームページのURL	
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： omniauth-shibboleth 研究開発国： 日本 研究開発時期： 平成24年5月～	すでにオープンソースとして公開済。 https://github.com/toyokazu/omniauth-shibboleth

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	○
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	佐賀大学理工学部
代表者名	理工学部長　渡　孝則
所在地	佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	
ホームページのURL	
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： 悪性Webサイトのマルチ環境解析システム 研究開発国： 日本 研究開発時期： 平成27年4月1日～	悪性Webサイトの分析手法と分析プログラムの基本部分はできている。悪性Webサイトの分析妨害技術が日々進化しているので、それに対応できるように、機能を拡張している。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	佐賀大学理工学部
代表者名	理工学部長　渡　孝則
所在地	佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	
ホームページのURL	
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： IoT機器向き軽量暗号認証方式 研究開発国： 日本 研究開発時期： 平成28年4月1日～	認証アルゴリズムの基本部分はできている。それをもとに暗号方式へと拡張を行っている。安全性の証明を行っている。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	○
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

イ　企業

企業・大学名	住友電気工業株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	
ホームページのURL	
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： 車載ネットワーク侵入検知技術の研究開発 研究開発国： 日本 研究開発時期： 平成27年10月1日～	車載ネットワーク通信に対するサイバー攻撃の検知アルゴリズムを開発。効果、性能を検証し、有効性を確認。市場導入に向け、実際の車輌に実装するための試作開発を実施中。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	