

# アクセス制御機能に関する技術の 研究開発の状況等に関する調査

## 調査報告書

平成 21 年 3 月

警察庁生活安全局情報技術犯罪対策課

# 第1章 調査の概要

## 1. 調査目的

不正アクセス行為の禁止等に関する法律において、国家公安委員会は、アクセス制御機能を有する特定電子計算機不正アクセス行為からの防御に資するため、毎年少なくとも1回、アクセス制御機能に関する技術の研究開発の状況を公表するものとされている。

本調査は、現在の研究開発の状況や実用化（製品化）されているアクセス制御機能等を把握することにより、不正アクセス行為からの防御に関する知識を普及させるとともに、今後の資料として活用しようとするものである。

## 2. 調査対象と調査方法

調査対象：以下に該当する調査対象から無作為に1,300件抽出した。

- 企業（800社）  
業種分類が「情報・通信」「サービス」「電気機器」「金融」である上場企業及び未上場企業
  - 大学（500校）  
国立・私立大学のうち、理工系学部を設置するもの
- 調査方法は、調査対象に対して調査票を送付し、期日までに回答を求める「郵送調査」方式を採用した。（調査期間：2008年12月15日～2009年1月16日）

## 3. 調査内容

本調査では次の二つを調査した。

### (1) 研究開発の傾向

アクセス制御機能に関する技術サービスの研究開発の傾向を分析するために、アクセス制御機能を7つの分野に分類し、企業や大学において力を入れている分野等を調査した。

調査票：付録資料にある『回答用紙A』を参照

【分類の表】

大分類	小分類
暗号	暗号技術、暗号化ソフト
認証	ワンタイムパスワード <sup>1)</sup> 、ICカード <sup>2)</sup> 、バイオメトリクス、PKI、アクセスコントロール(シングルサインオン含む)
ネットワークセキュリティ	ファイアウォール、VPN、フィルタリング <sup>3)</sup> 、コンテンツセキュリティ
不正侵入対策	侵入検知 (IDS)、追跡
セキュリティマネジメント	ログ解析、資産管理、情報保護、セキュリティ情報管理
ウイルス対策ツール	ウイルス対策ソフト
セキュリティサービス関連	セキュリティ診断、不正アクセス監視、ウイルス等監視、認証サービス、セキュリティコンサルティング <sup>4)</sup>

## (2) 実用化された製品及び研究開発中の技術・サービス

既に実用化された個々の製品（ハードウェア、ソフトウェア、サービス）及び現在開発中の個々の技術・サービスの内容について調査した。

調査票：付録資料の『回答用紙B』『回答用紙C』を参照

## 4. 送付・回収状況、集計対象件数

※ 送付数・回収数・回収率

	送付数	回収数	回収率 (%)
企業	800	102	12.8%
大学	500	113	22.6%
合計	1300	215	16.5%

※ 各回答用紙別の集計対象件数

	回答用紙A	回答用紙B	回答用紙C
企業	102	9	6
大学	113	7	47
合計	215	16	53

## 5. 報告書を見る際の留意点

- ・ 集計結果の比率は、小数点第二位を四捨五入し、少数第一位までを百分率（%）で表示している。
- ・ 選択肢から1つだけ選んで回答する設問では、構成比の和が100.0%にならないことがある。
- ・ 本文やグラフ中の選択肢は、調査票の言葉を短縮しているものがある。
- ・ 回答件数が少ないものについては、コメントの対象としていない。
- ・ 調査対象の条件が平成18年度以前の調査と異なっているため、経年変化のデータについては特に留意が必要である。

※ 平成18年度（一昨年度）の調査対象：

アクセス制御機能に関する技術の研究開発を行っていると思われる企業や大学から500件抽出。

企業：企業・団体から無作為に抽出

大学：国立・私立大学の理工系・情報系の学部・大学院および研究所等から無作為に抽出

※ 平成19年度以降の調査対象：

以下に該当する企業や大学から、平成19年度は600件、平成20年度は1,300件を無作為に抽出。

企業：「情報・通信」「サービス」「電気機器」「金融」である上場企業及び末上場企業

大学：国立・私立大学のうち、理工系学部を設置するもの

## 第2章 調査結果（概要と考察）

### 1. 研究開発の傾向

『回答用紙A』により調査した研究開発の傾向について、過去との比較を含めて考察した。

#### (1) 研究開発体制・売り上げ

企業・大学ともに昨年同様、小規模な開発が主流になっているが、企業では費用面での中～大規模開発が昨年度より増加していることが確認できる。

研究開発人員をみると、全体ベースでは、「1～4人」の小規模人員が主流となっている。

企業・大学別にみると、企業については、「1～4人」「5～9人」の層が最多だが、大規模人員層にも一定数の回答が確認できる。大学については、「1～4人」が最多でかつ、昨年度よりも割合が高まっているが、一方で「20～49人」「100人以上」の層も増加している。企業・大学とも小規模人員が主流ではあるものの、一概に開発人員が減少しているとは捉えられない。（23～27ページ参照）

また、研究開発費についてみると、全体では「～1,000万円未満」～「10億～100億円未満」まで幅広く分布していることが確認できる。

企業・大学別にみると、企業については、「1,000万～1億円未満」「1億～10億円未満」層の研究開発が昨年度と比べて増加している。大学については、「～1,000万円未満」層の割合が昨年度よりさらに高くなっており、小規模開発が主流になっていることがうかがえる。（28～32ページ参照）

## (2) アクセス制御機能に関する技術研究開発に係る現状と今後の展望

昨年に引き続き、「ネットワークセキュリティ」についての研究開発意欲が企業・大学ともに高い傾向がうかがえる。企業における開発分野は比較的幅広いが、大学においては、「認証技術」「セキュリティマネジメント」「不正侵入対策」等の研究開発に集約される。

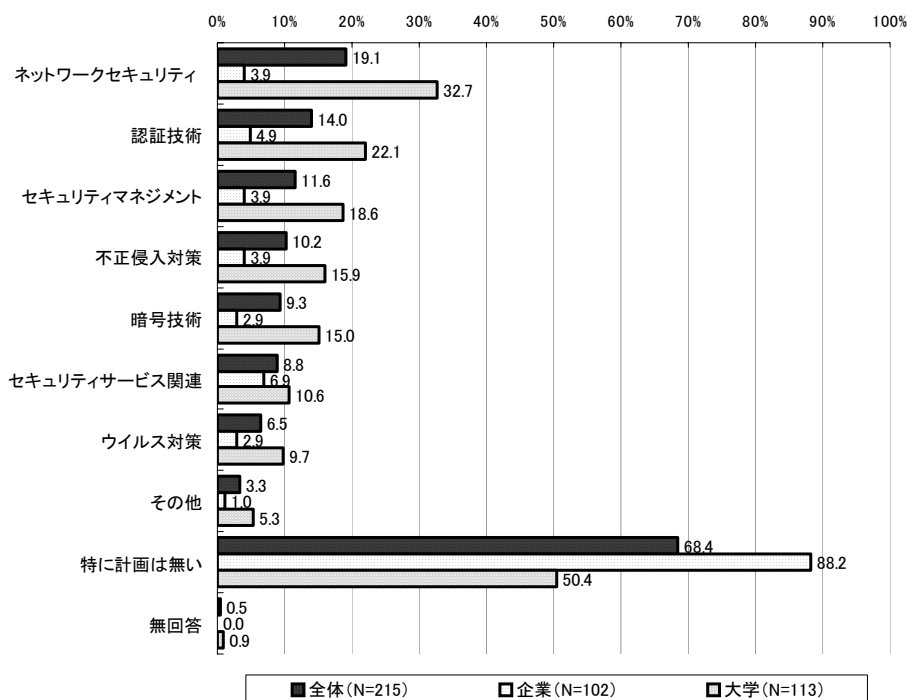
“現在取り組んでいる分野”としては、割合の高い順に「ネットワークセキュリティ」「認証技術」「不正侵入対策」となっており、いずれも昨年度と同様に上位項目に位置している。この傾向は企業・大学ごとにみても同様の傾向にある。昨今増え続けているウェブ経由の脅威や脆弱性に対する攻撃から守る技術開発の必要性が、近年、より高まっているものと考えられる。(38～42 ページ参照)

また、“今後の取り組み予定分野”についてみると、全体ベースでは「ネットワークセキュリティ」が昨年度と同様に最も高く、続いて「認証技術」「セキュリティマネジメント」「不正侵入対策」等の技術開発が挙げられている。

企業については、「認証技術」「暗号技術」「ネットワークセキュリティ」といったスタンダードな技術開発から、「セキュリティマネジメント」や「セキュリティサービス」といったIT全般統制の為のツールやサービスまで幅広く分布している。基本的な技術が確立し、競争が激化した現在のセキュリティ市場においては、より低コストでよりの確な技術を開発していく必要があり、今後の研究開発は、幅広く細分化していくものと考えられる。

大学については、「ネットワークセキュリティ」「認証技術」「セキュリティマネジメント」等が上位分野となっている。関係者以外の不特定多数が行き来する大学においては、キャンパス内認証のほか、データのみならず人や物を統合的に管理する様なセキュリティシステムに開発も求められるなど、より確かな認証技術、ネットワーク管理が必要となっている。(43～47 ページ参照)

- 今後、取り組んでいく分野 -



### (3) アクセス制御機能に関する実用化（製品化）に係る現状と今後の展望

アクセス制御機能の実用化（製品化）については、今後においても、より実用度が高く、より安全なセキュリティ技術の開発が求められていくものと考えられる。

“現在、実用化（製品化）されているアクセス制御機能” についての質問では、「実用化されているものは無い」が 80%弱を占める結果となった。回答があったものをみると、割合の高い順に「認証技術」「ネットワークセキュリティ」「ウイルス対策」となっている。

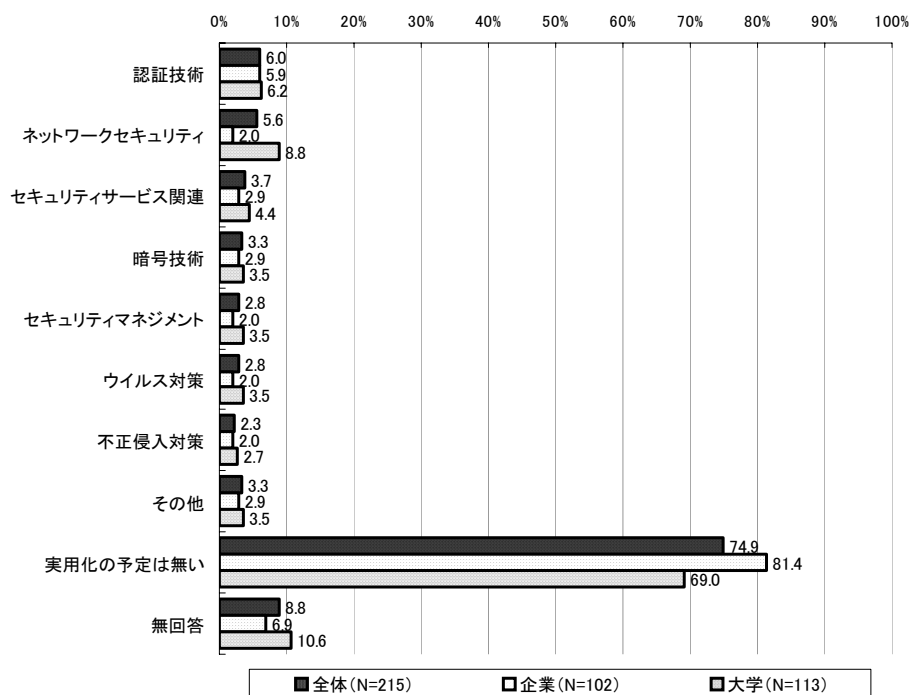
（53～57 ページ参照）

“今後実用化（製品化）を見込んでいるもの” については、全体ベースでは「認証技術」「ネットワークセキュリティ」「セキュリティサービス関連」の順となっており、現在実用化されているものとほぼ同様であり、また昨年度とも同様の傾向となっている。（58～62 ページ参照）

“今後、最も力を入れていく分野” については、全体ベースでは「ネットワークセキュリティ」「認証技術」「セキュリティサービス関連」の順となっており、「セキュリティマネジメント」は、企業における“今後実用化（製品化）を見込んでいるもの”での割合が低かったものの、“力を入れていく分野”では上位にあり、今後重要になってくる項目であると推察される。（48～52 ページ参照）

以上により、今後実用化（製品化）を見込んでいるアクセス制御機能としては、「ネットワークセキュリティ」や「認証技術」「セキュリティサービス関連」といった、情報セキュリティにおいてはスタンダードな分野が実用化（製品化）の中心となっている。

- 今後、実用化（製品化）を見込んでいるアクセス制御機能 -



## 2. 実用化された製品及び研究開発中の技術・サービス

### 2.1 研究開発・製品化事例の考察

『回答用紙B』『回答用紙C』により調査した、研究開発中および実用化された技術・サービスの動向について考察した。調査項目は、下記の内容について複数選択で聞いている。

(1) 何を守るか？

- ・どのコンポーネントを守るのか、という観点から見た分類。
- ・ネットワーク、サーバ、クライアントなどの大きな括りの視点で見ると見る。

(2) 何かから保護するか？

- ・どのような脅威から守るのか、という観点から見た分類。
- ・買う側の立場からみて、どのような対策をしたいかという視点でもある。

(3) どのような機能を持っているか？

- ・どのような技術要素を使って守るのか、という観点から見た分類
- ・売る側や開発する側の立場から見た、機能要素という視点でもある。

(4) どのようなセキュリティ上の効果があるか？

- ・どのような効果を狙ったものか、という観点から見た分類。
- ・事前対応、事中・事後対応という視点でもある。

(5) どのようなレイヤーのセキュリティを守るか？

- ・どのようなレイヤーでセキュリティを守るのか、という観点から見た分類。

(6) どのようなサービスか？

- ・サービスの場合、どのような内容か、という観点から見た分類。

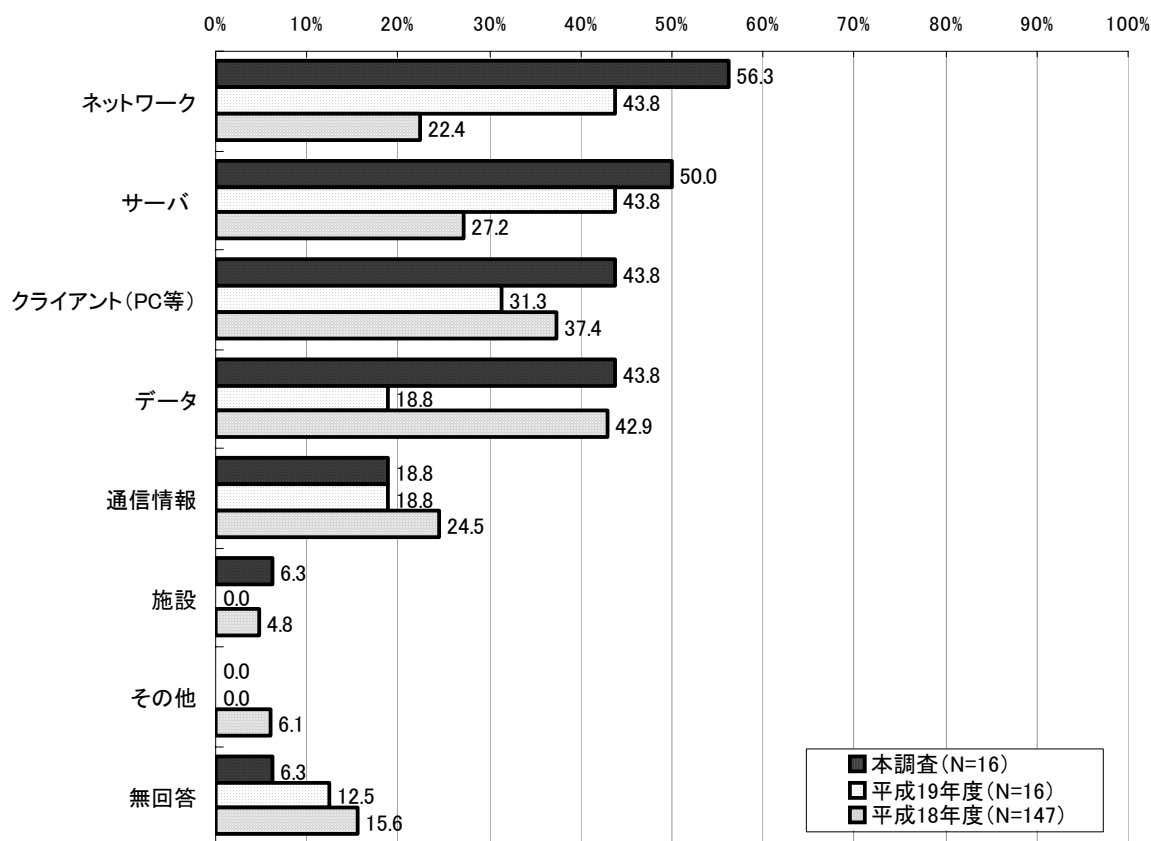
## (1) 何を守るか？

### ① 実用化（製品化）されているもの

「何を守るか？」という視点からみた実用化（製品化）されている分野については、昨年度と同様、「ネットワーク」を守るものが56.3%（9件）と最も高く、次いで「サーバ」を守るものが50.0%（8件）、「クライアント（PC等）」「データ」を守るものが共に43.8%（7件）で続いている。近年増え続けているウェブ経由の脅威や、脆弱性に対する攻撃から守る製品の開発は、今後も引き続き進められていくものと考えられる。

#### 【経年変化】何を守るか？

##### ① 実用化（製品化）されているもの(MA)



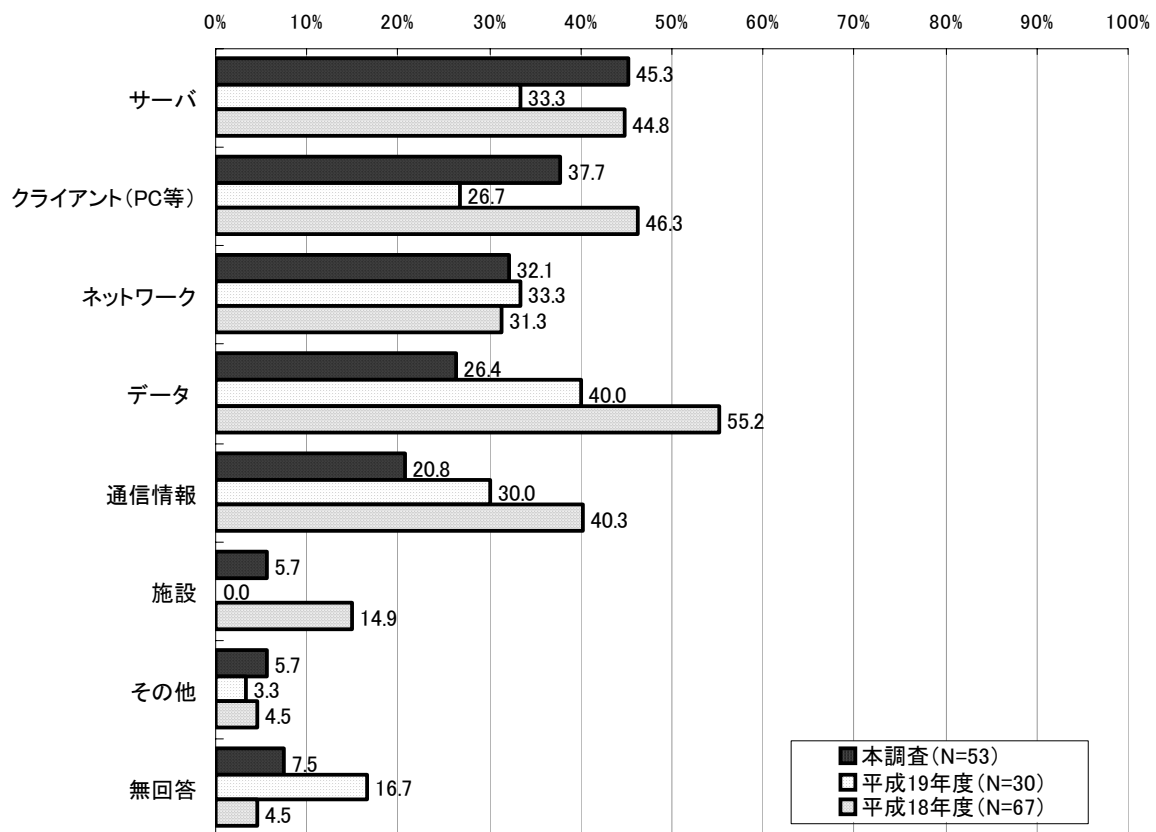


## ②研究開発中のもの

研究開発中のものでは、「サーバ」を守るものの割合が 45.3%（24 件）と最も高い。次いで「クライアント（PC 等）」を守るものが 37.7%（20 件）、「ネットワーク」を守るものが 32.1%（17 件）と続く。

実用化（製品化）されているものと同様、ネットワークやサーバを強化し、データやクライアント（PC 等）への攻撃からの対策が重要となってきた。

【経年変化】何を守るか？  
②研究開発中のもの(MA)



## (2) 何から保護するか？

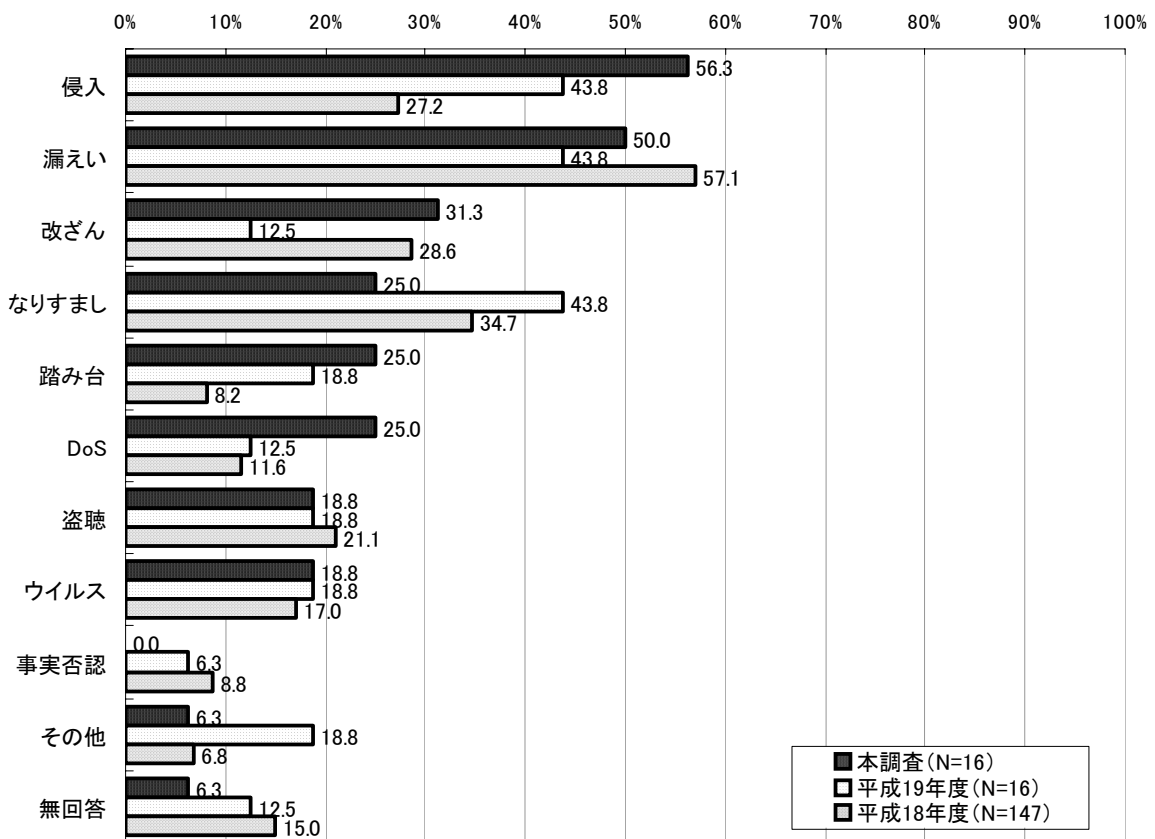
### ① 実用化（製品化）されているもの

「何から保護するか？」という視点でみていくと、「侵入」が 56.3%（9 件）と最も割合が高く、次いで「漏えい」が 50.0%（8 件）、「改ざん」が 31.3%（5 件）と続く。

近年においては、企業にとっては攻撃対策よりも“情報漏えい”対策がより必要なものと捉えられている。

【経年変化】何から保護するか？

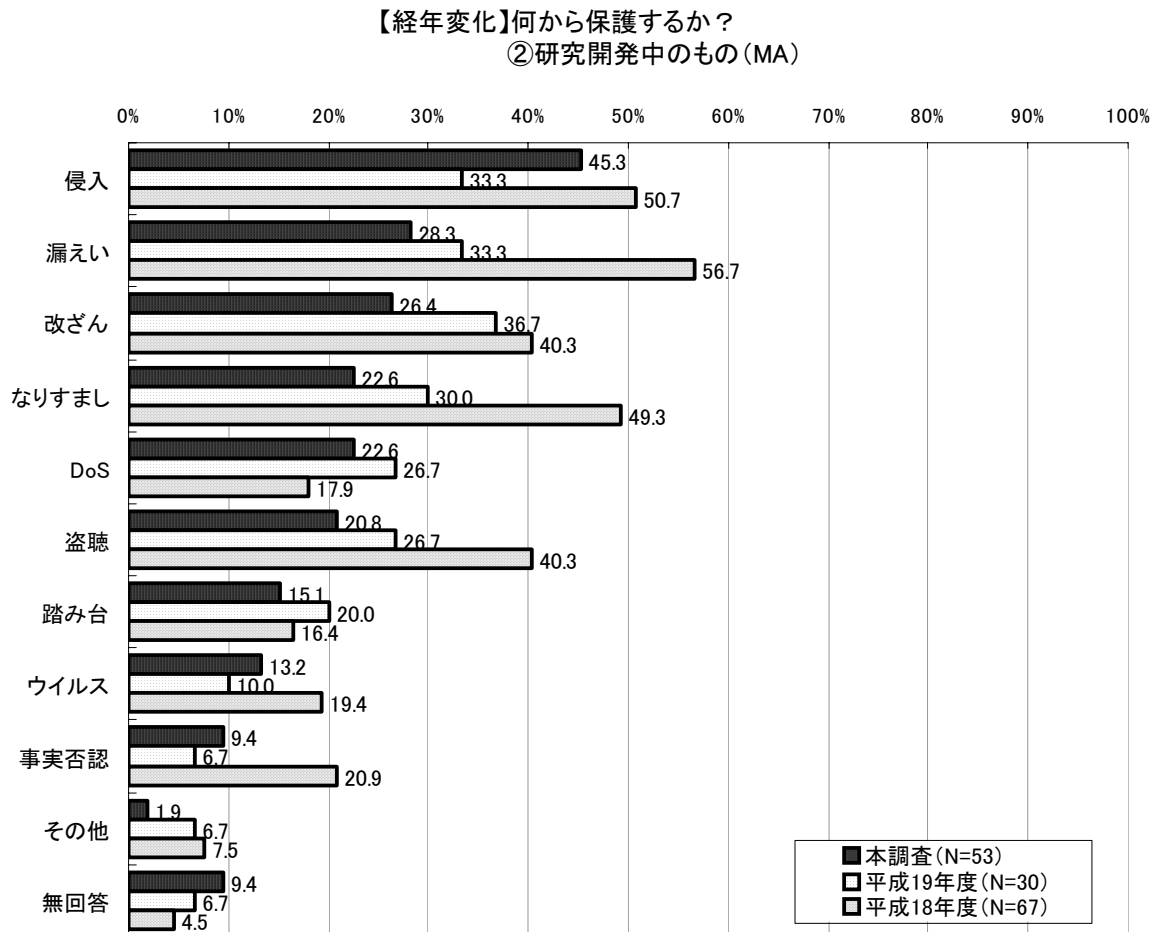
① 実用化（製品化）されているもの（MA）



## ②研究開発中のもの

研究開発中ものについては、「侵入」が45.3%（24件）と最も割合が高く、次いで「漏えい」が28.3%（15件）、「改ざん」が26.4%（14件）と続く。

上位の項目は、昨年度と比べて同様の傾向であり、引き続き“情報漏えい”対策に注力がされている傾向が見受けられる。



### (3) どのような機能を持つか？

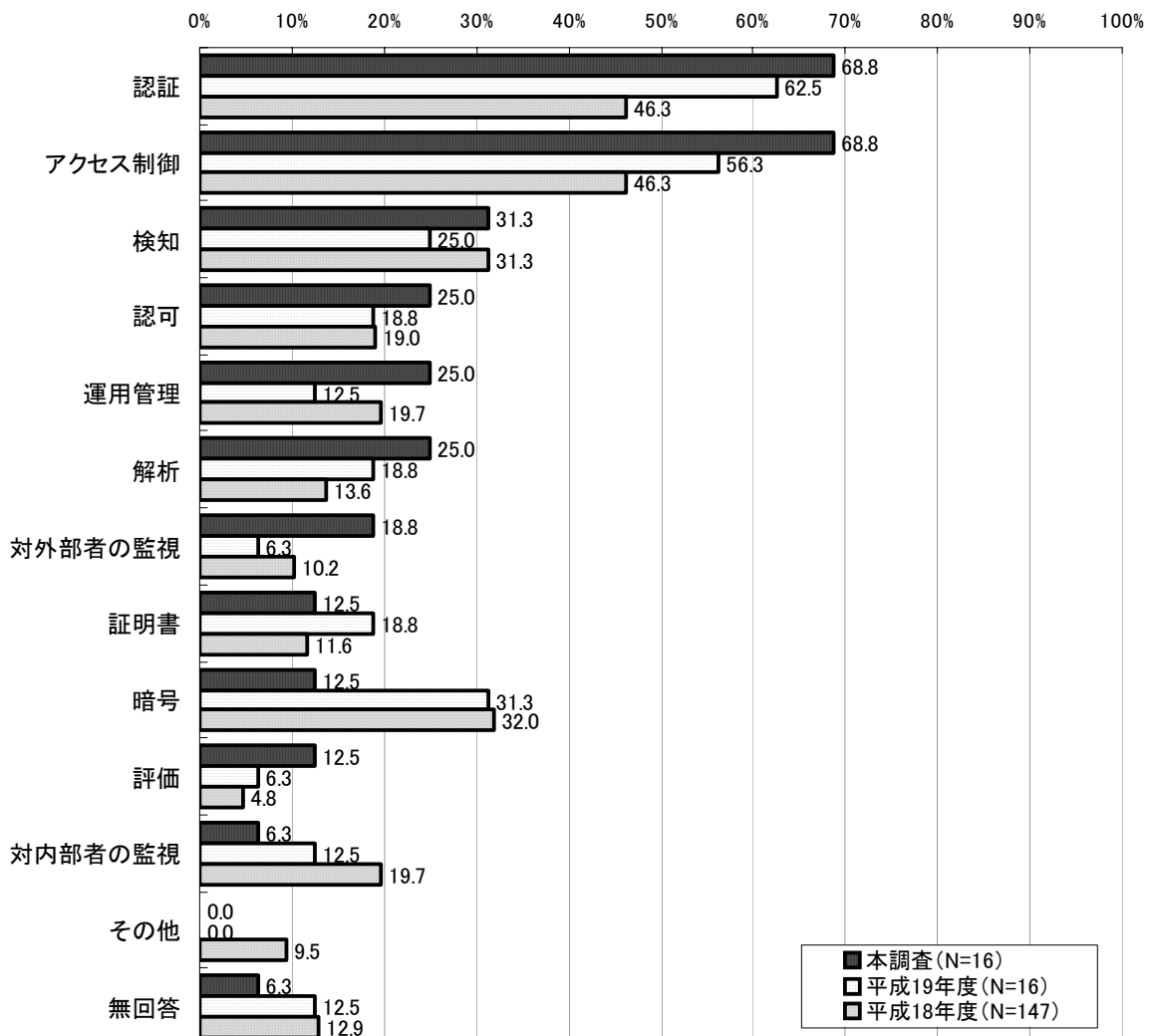
#### ① 実用化（製品化）されているもの

実用化（製品化）されている機能としては、「認証」と「アクセス制御」が共に 68.8%（11 件）と割合が最も高く、次いで「検知」が 31.3%（5 件）、「認可」が 25.0%（4 件）と続いている。

昨年度と同様、情報漏えい対策の主流となる機能を中心に研究開発が進められている様相がうかがえる。

【経年変化】どのような機能を持つか？

①実用化（製品化）されているもの(MA)

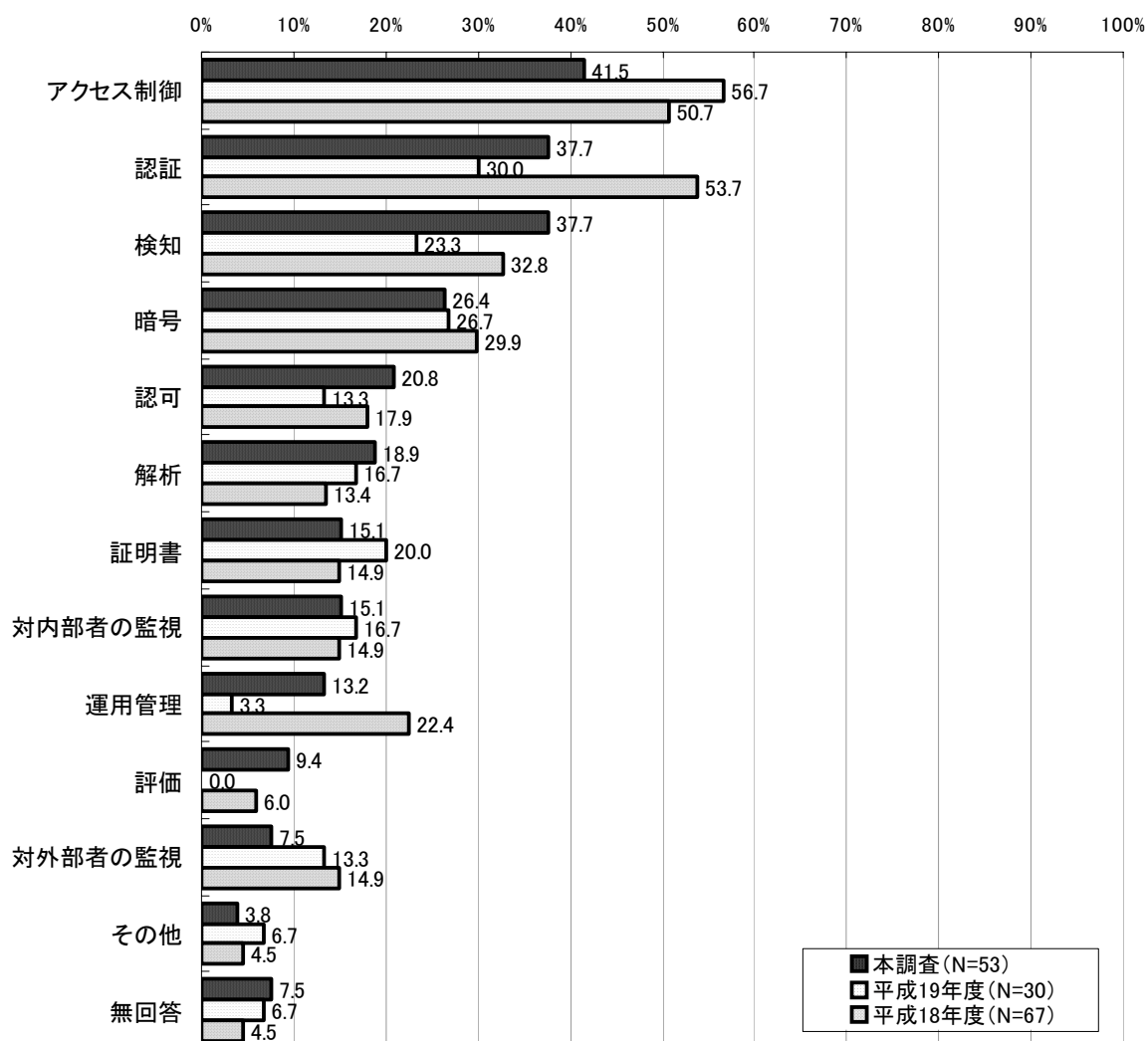


## ② 研究開発中のもの

研究開発中のものでは、「アクセス制御」が41.5%（22件）と割合が最も高く、次いで「認証」と「検知」が共に37.7%（20件）、「暗号」が26.4%（14件）と続く。

昨年度に比べて上位の項目に大きな変化は見られず、近年の「アクセス制御」に対する重要性の急速な高まりが改めて確認できる。

【経年変化】どのような機能を持つか？  
②研究開発中のもの(MA)

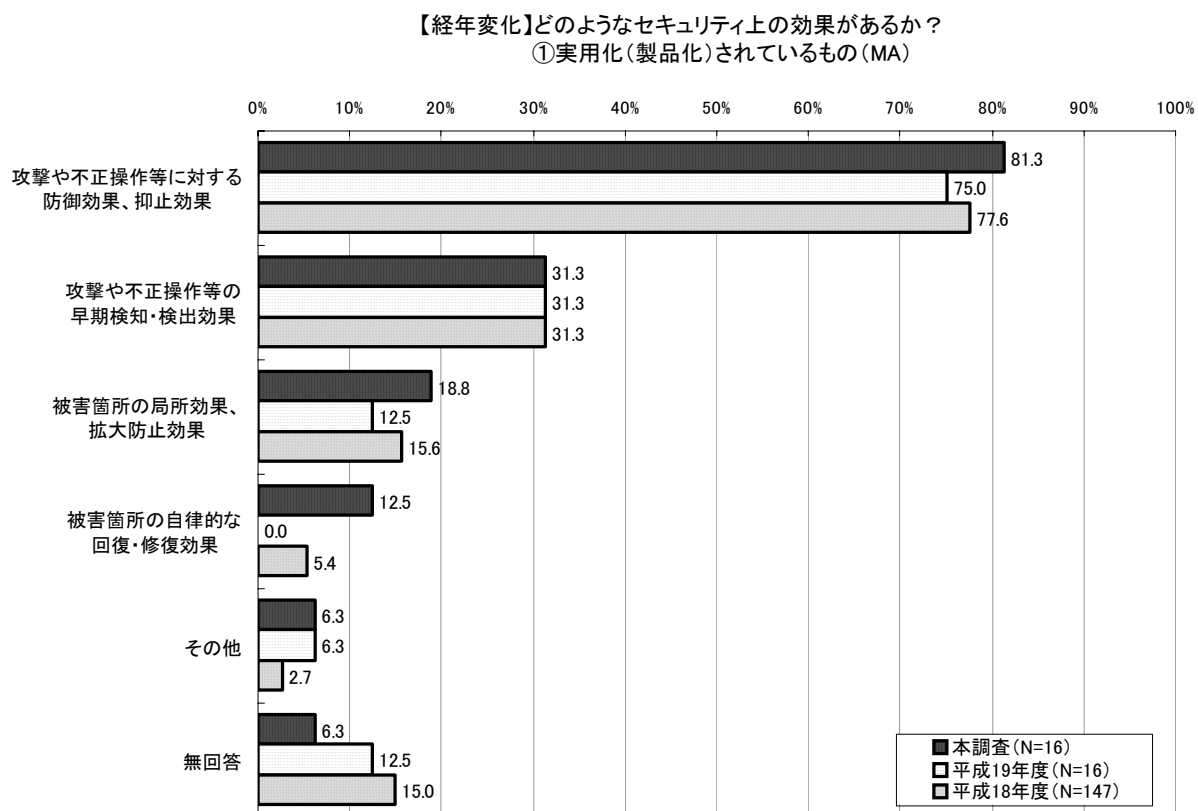


#### (4) どのようなセキュリティ上の効果があるか？

##### ① 実用化（製品化）されているもの

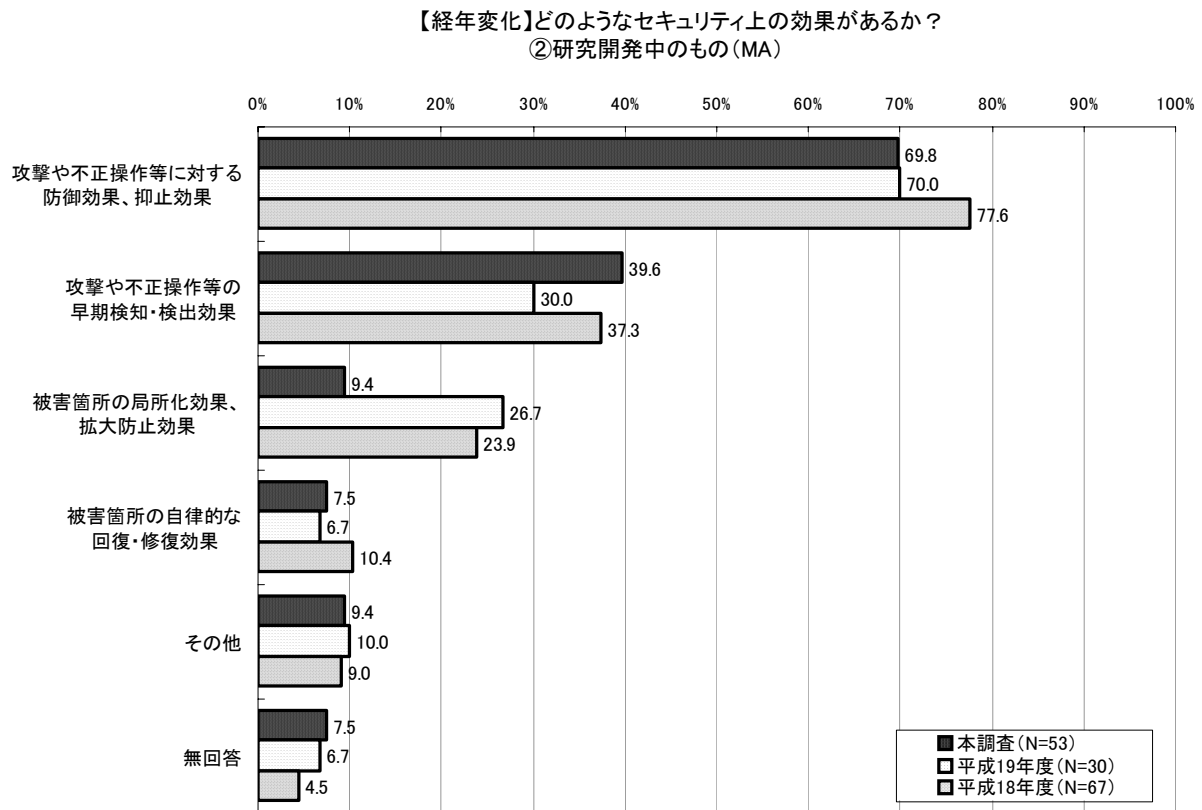
セキュリティ上の効果としては、「攻撃や不正操作等に対する防御効果、抑止効果」の割合が 81.3%（13 件）と他の効果と比べて非常に高く、一昨年来から同様の傾向で推移している。

まずは攻撃や不正操作等による被害を絶対に起こさせないことが、企業の情報セキュリティ対策の使命として重要となっていることが見て取れる。



## ② 研究開発中のもの

研究開発中のものでは、実用化（製品化）されているものと同様、「攻撃や不正操作等に対する防御効果、抑止効果」が69.8%（37件）で最も多い。



## (5) どのようなレイヤーのセキュリティを守りますか？

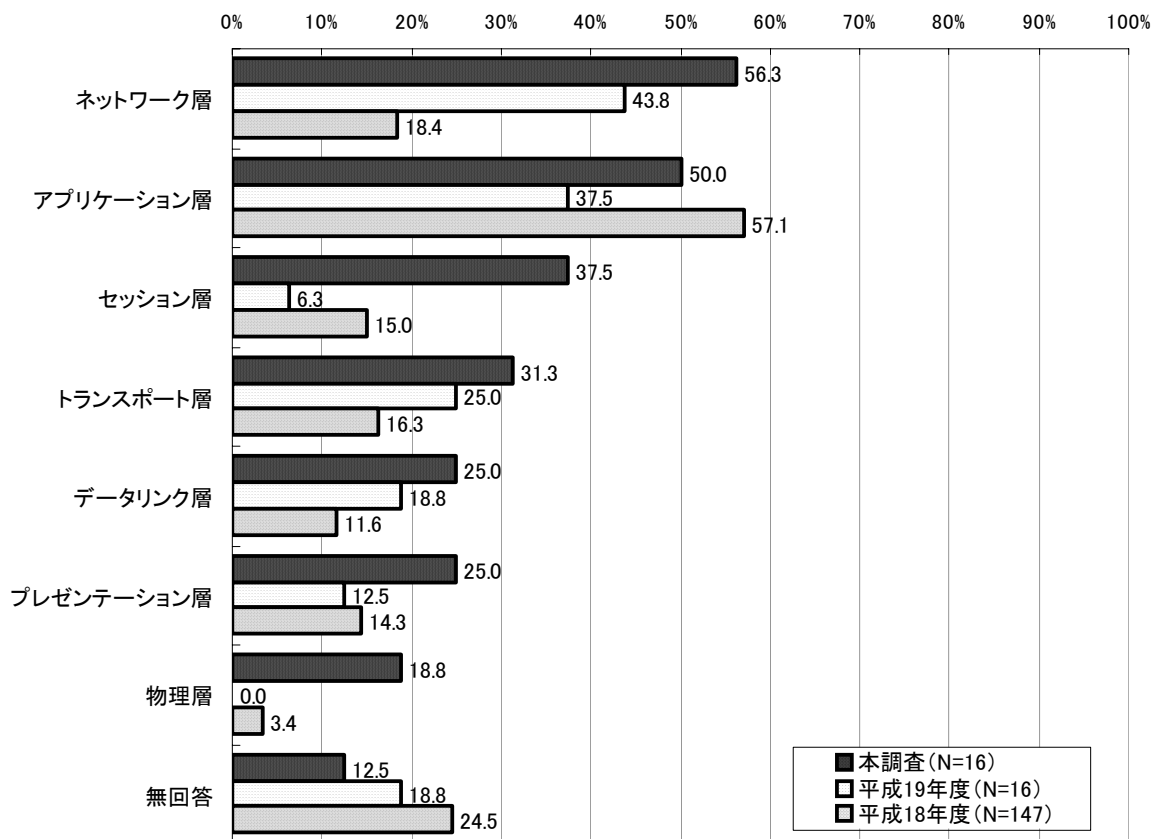
### ① 実用化（製品化）されているもの

セキュリティを守るレイヤーとしては、割合が高い順に、「ネットワーク層」が56.3%（9件）、「アプリケーション層」が50.0%（8件）となっている。また昨年度と比べ「セッション層」の割合が大きく増えている。

情報セキュリティ対策において、ネットワーク層やアプリケーション層に対する研究開発が近年の主流である事がうかがえる。

【経年変化】どのようなレイヤーのセキュリティを守りますか？

①実用化（製品化）されているもの(MA)

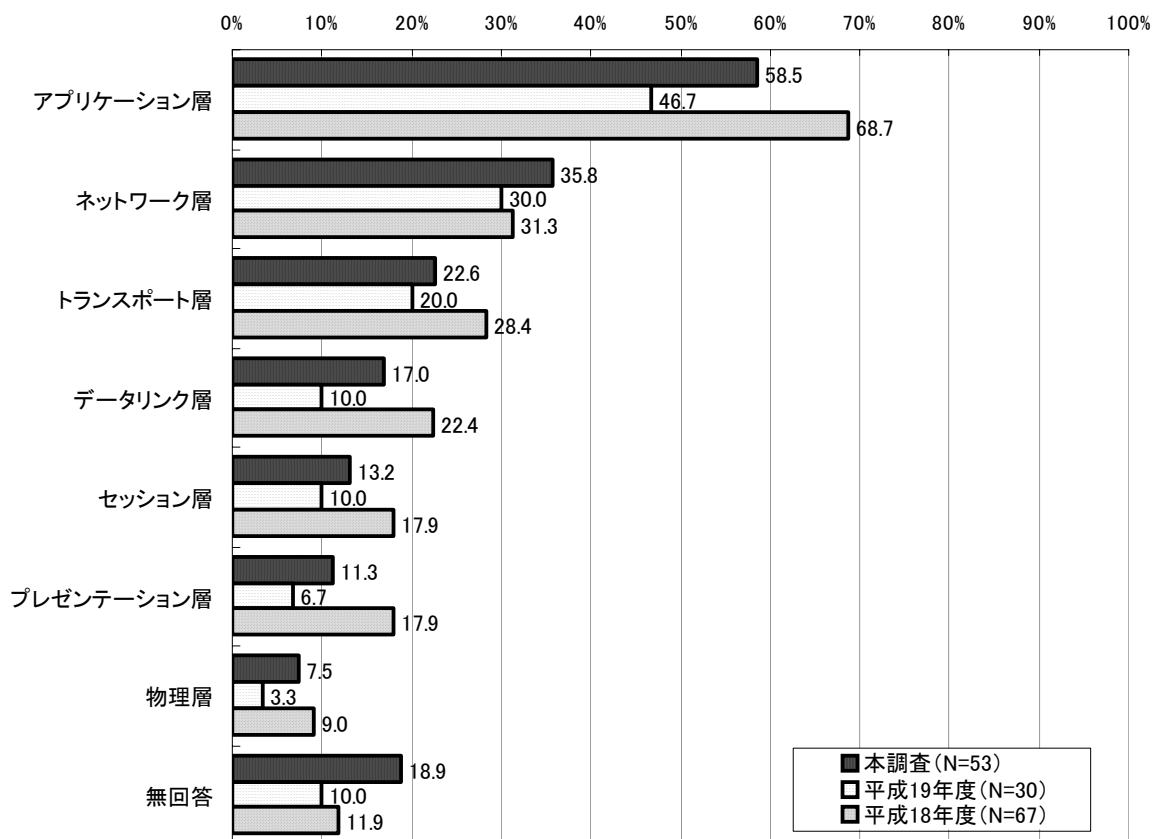




## ② 研究開発中のもの

研究開発中のものでは、昨年度と同様、「アプリケーション層」が最多で58.5%（31件）となっている。次いで「ネットワーク層」が35.8%（19件）と続く。

【経年変化】どのようなレイヤーのセキュリティを守りますか？  
②研究開発中のもの(MA)



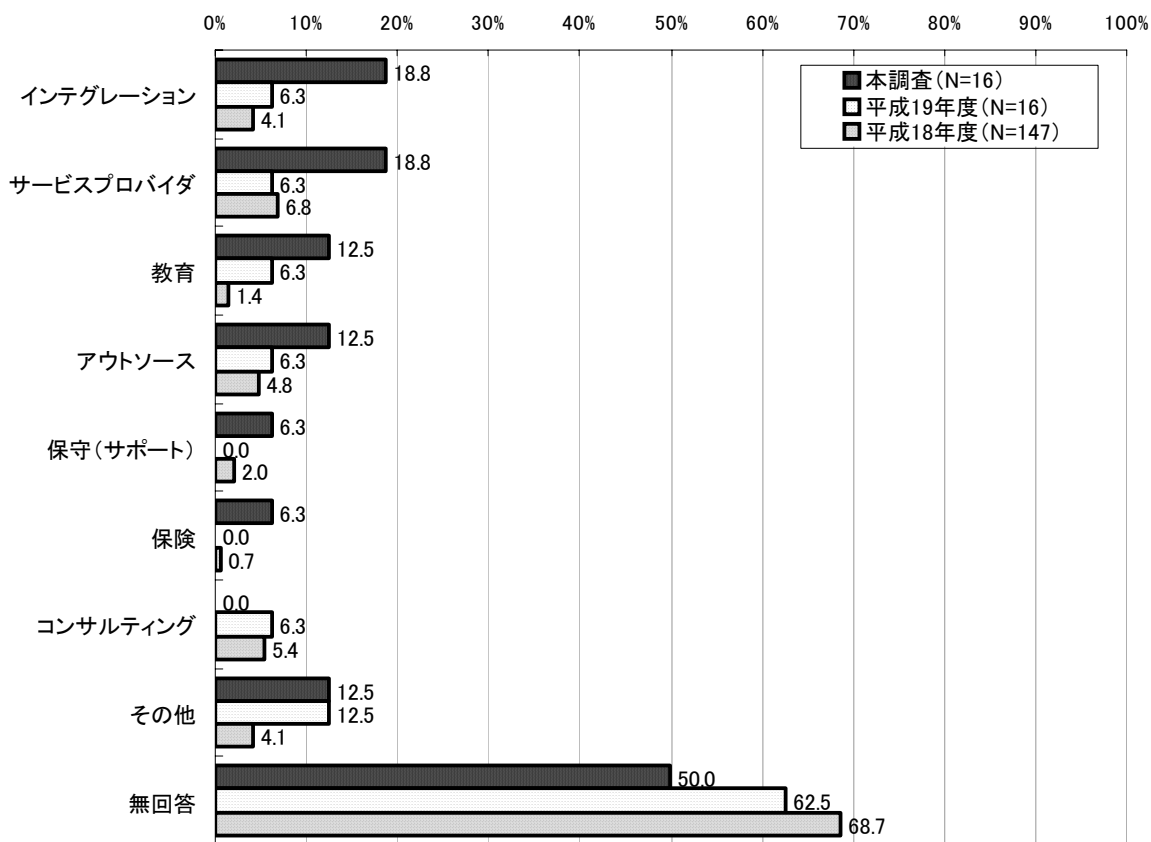
## (6) どのようなサービスか？

### ① 実用化（製品化）されているもの

サービスについては、昨年度同様、無回答の割合が高いものの、大部分のサービスにおいて、昨年度よりも相対的に割合が高くなっている。「インテグレーション」と「サービスプロバイダ」が共に18.8%（3件）と最上位となっている。

【経年変化】どのようなサービスか？

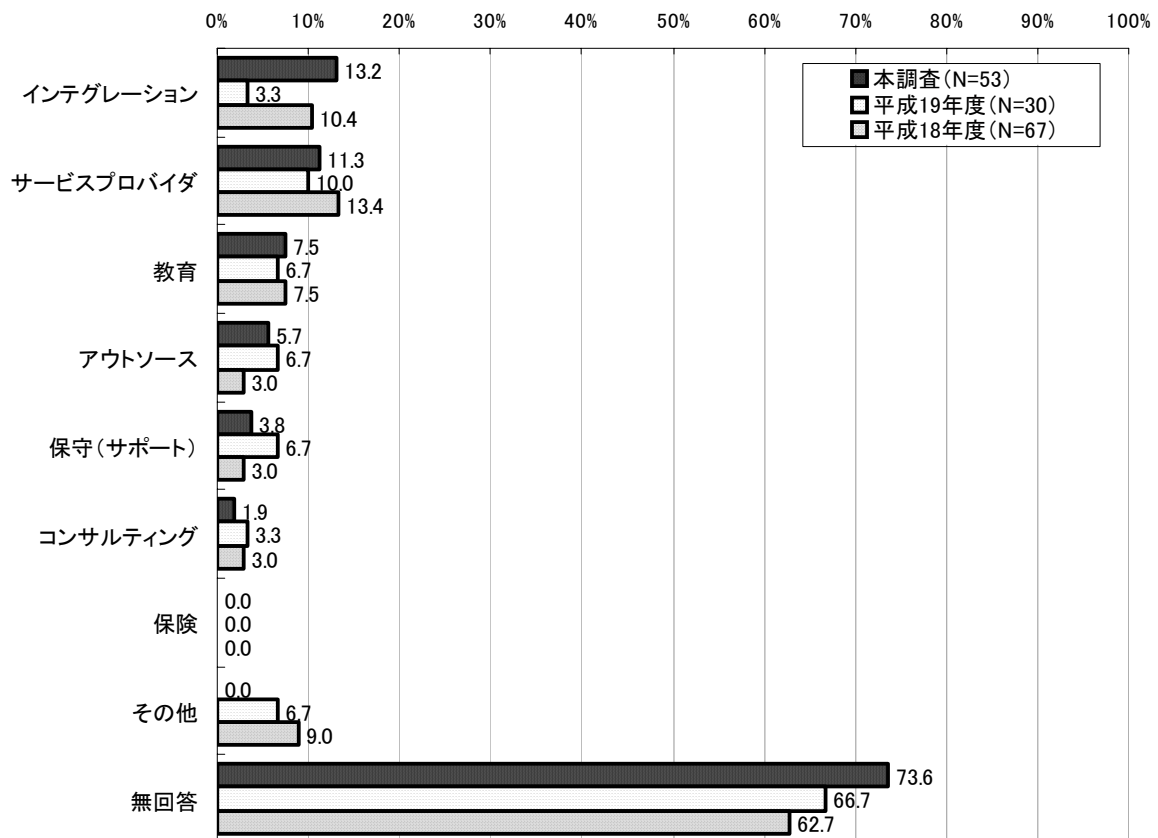
①実用化（製品化）されているもの(MA)



## ② 研究開発中のもの

先に述べた実用化（製品化）されているものと同様、「無回答」の割合が高いものの、「インテグレーション」「サービスプロバイダ」「教育」等では昨年よりも相対的に割合が高くなっている。最上位の「インテグレーション」が 13.2%（7 件）、次いで「サービスプロバイダ」が 11.3%（6 件）で続いている。

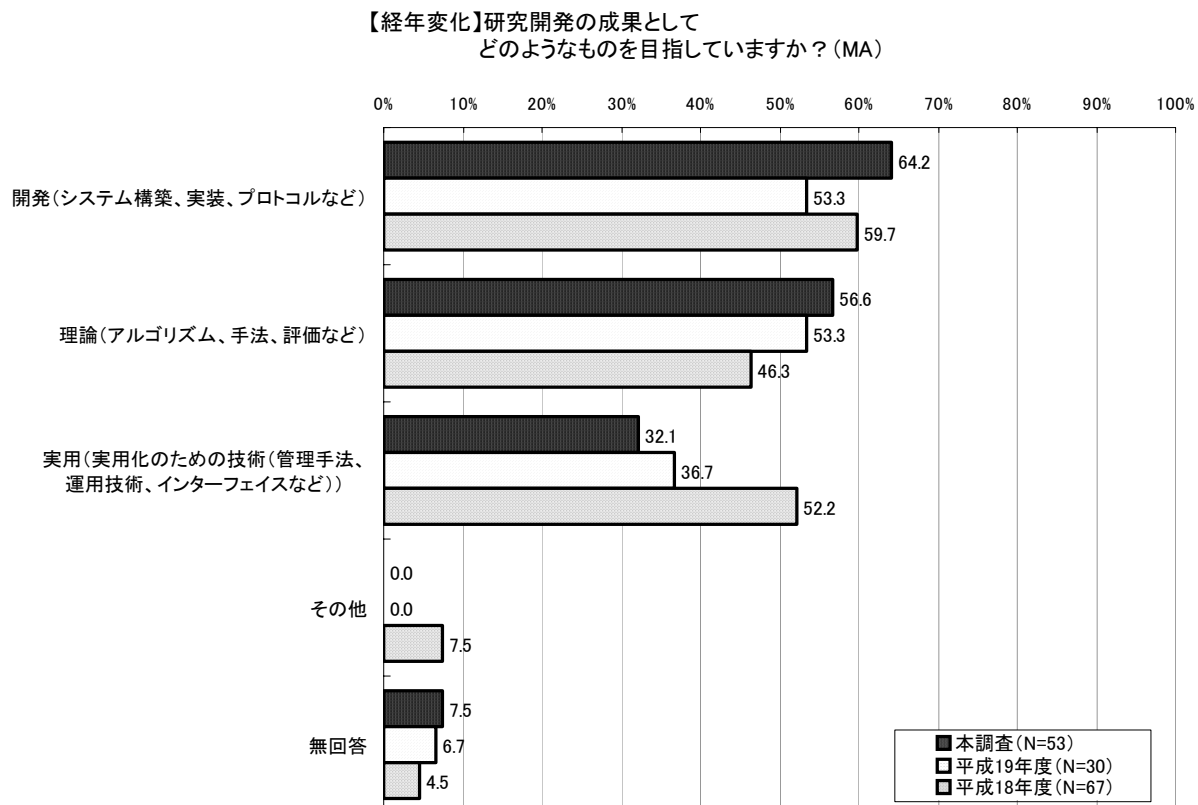
【経年変化】どのようなサービスか？  
②研究開発中のもの(MA)



## (7) 研究開発の成果としてどのようなものを目指していますか？

研究開発成果の技術レベルについてみると、開発レベルが64.2%（34件）、理論レベルが56.6%（30件）とそれぞれ割合は昨年度と比べ、増加している。

一方で実用化のための研究開発が昨年度と比べさらに減っているが、昨年度同様、今回調査においても大学からの回答が多数を占めたことが背景にあり、特に実用レベルの研究が減少しているとは捉えられない。

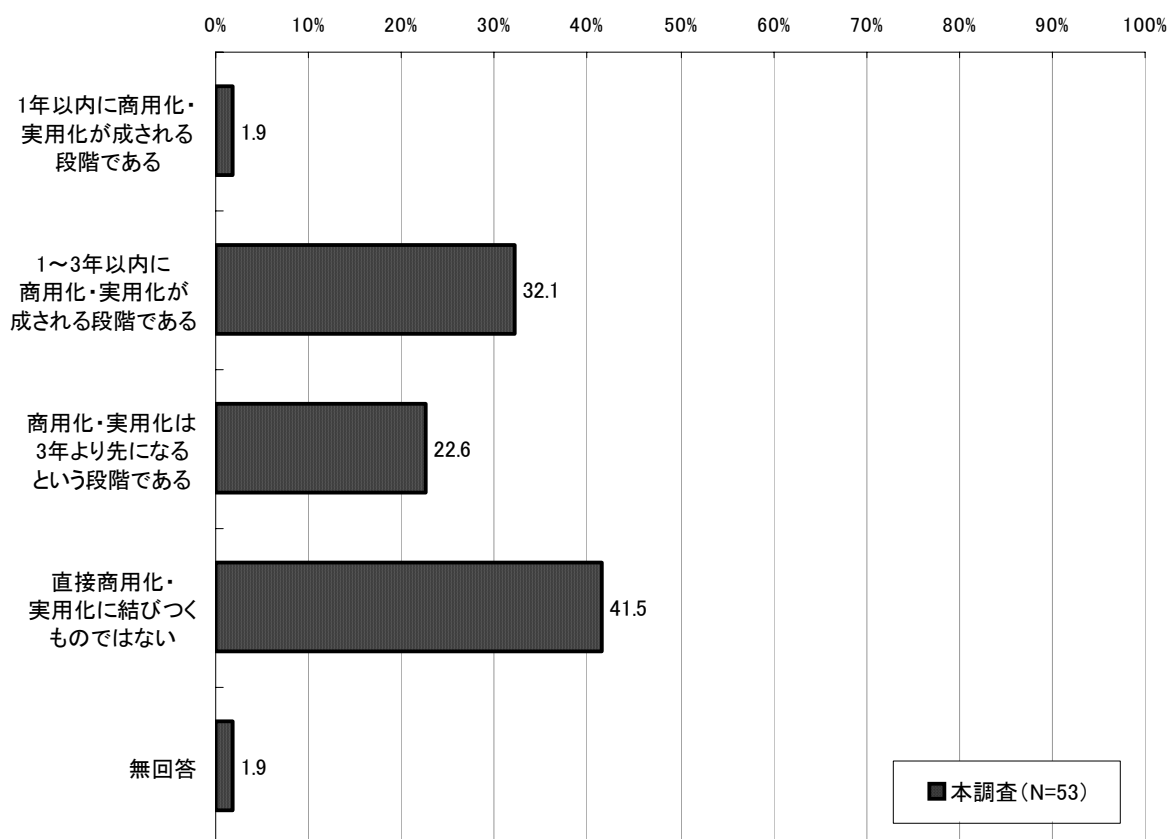


## (8) 研究開発の進捗状況

「直接商用化・実用化に結びつくものではない」が 41.5%（22 件）で最多となっているが、今回調査では企業からの回答が少なかったことが背景と言える。

現在研究開発中のものでは、「1～3 年以内」に商用化・実用化を目指しているものが 32.1%（17 件）で最多となっている。

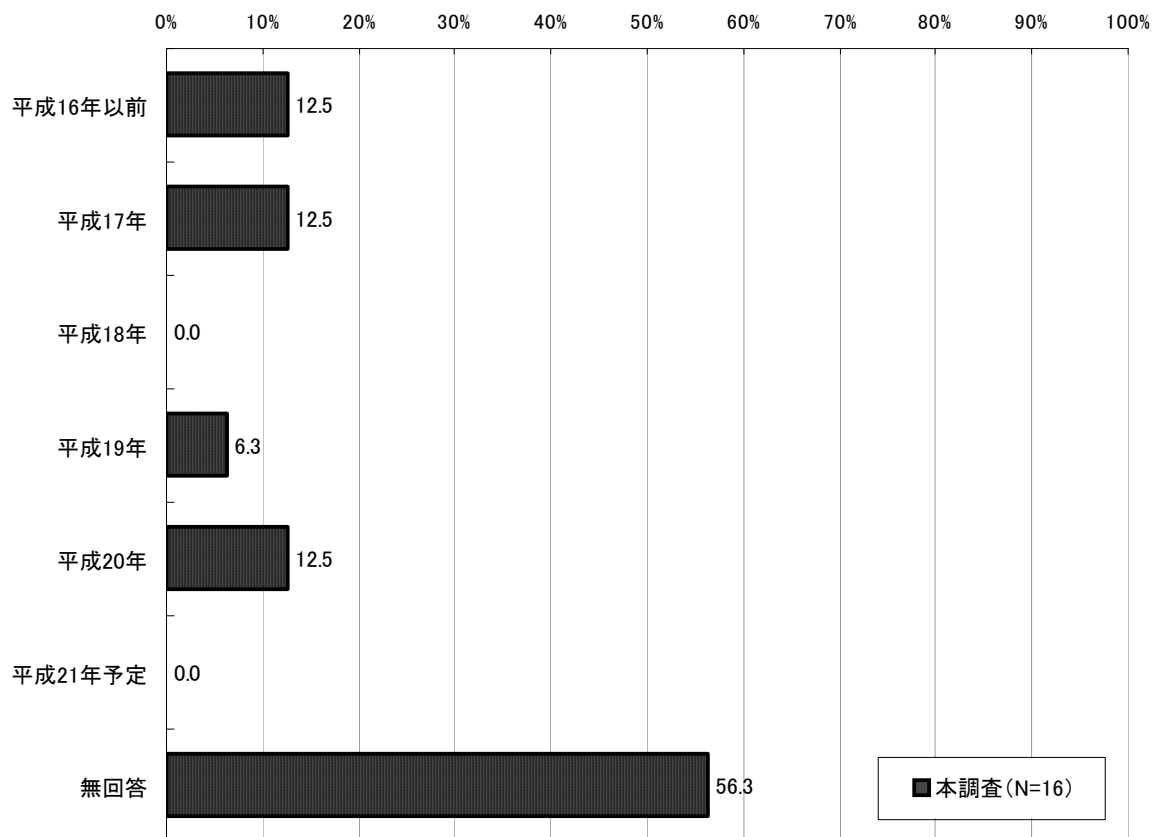
【全体】研究開発の進捗状況(SA)



### (9) 発売時期の分布

発売時期についてみると、「平成16年以前」「平成17年」「平成20年」がそれぞれ12.5%（2件）となっている。

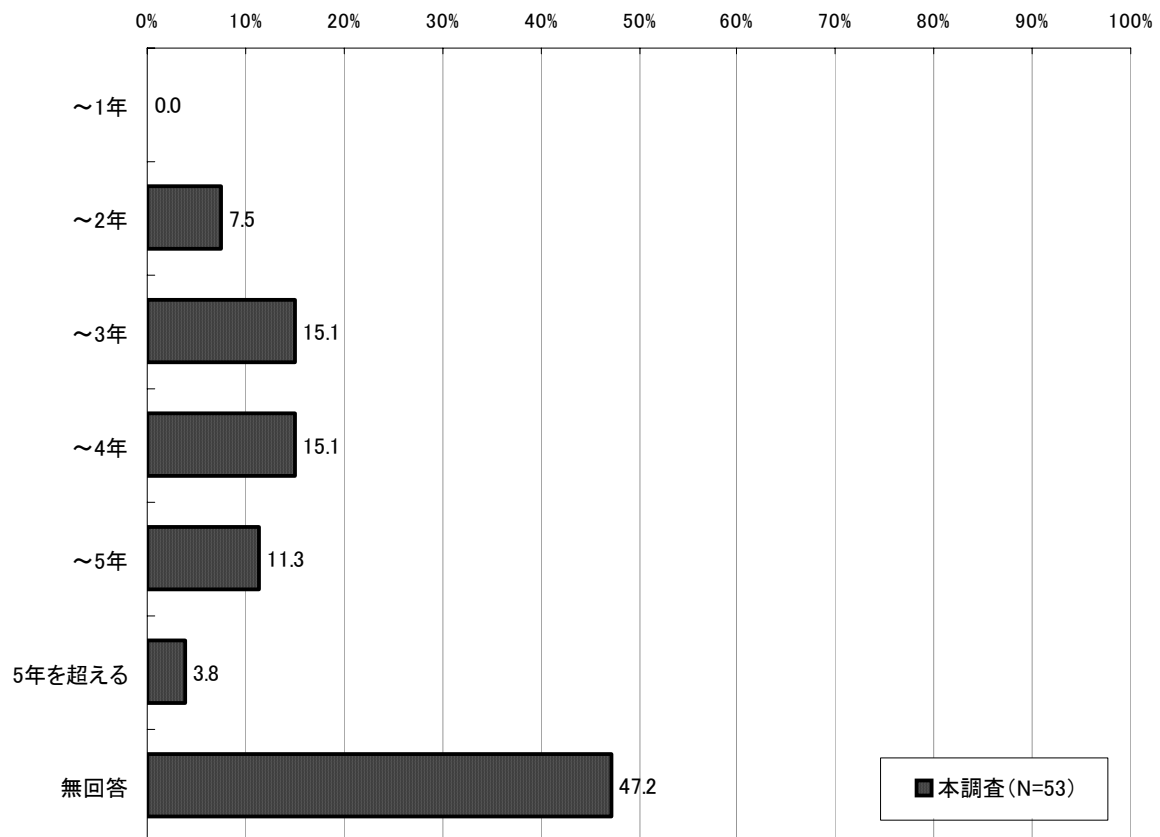
【全体】発売時期の分布(SA)



## (10) 研究開発期間の分布

研究開発期間をみると、「期間3年以内」と「期間4年以内」がそれぞれ15.1%（8件）づつで、最多となっている。

【全体】研究開発期間の分布(SA)



## 第3章 調査結果（データ）

### 1. 研究開発の傾向

『回答用紙A』により調査した研究開発の傾向について、個別データを示す。

#### 1.1 回答企業・大学の属性

##### (1) 研究開発に携わっている人数

###### 【本調査】

○企業、大学ともに「1～4人」の小規模人員が主流となっている。但し、大学では中～大規模人員を抱えるところも数は少ないが一定数確認できる。

###### 【経年比較】

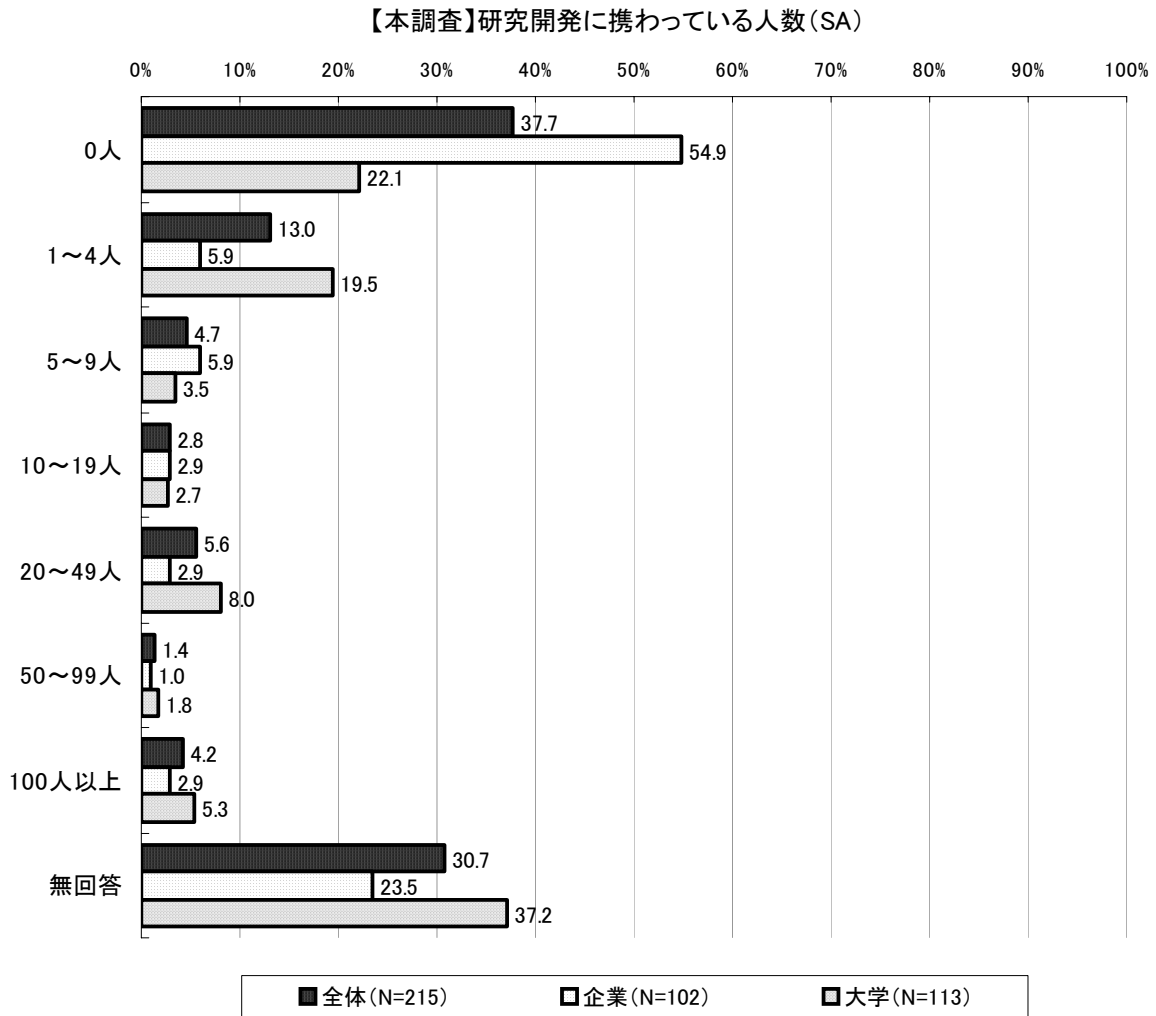
○企業においては、有効回答数が少なく傾向は捉えにくい。比較的小規模な人員構成が主流と考えられる。

○大学においては、昨年度に続き、「1～4人」の小規模人員層が最多となったものの、「20人以上」「100人以上」といった層も昨年度と比べて増加しており、一概に開発人員が減少しているとは捉えられない。



【本調査】

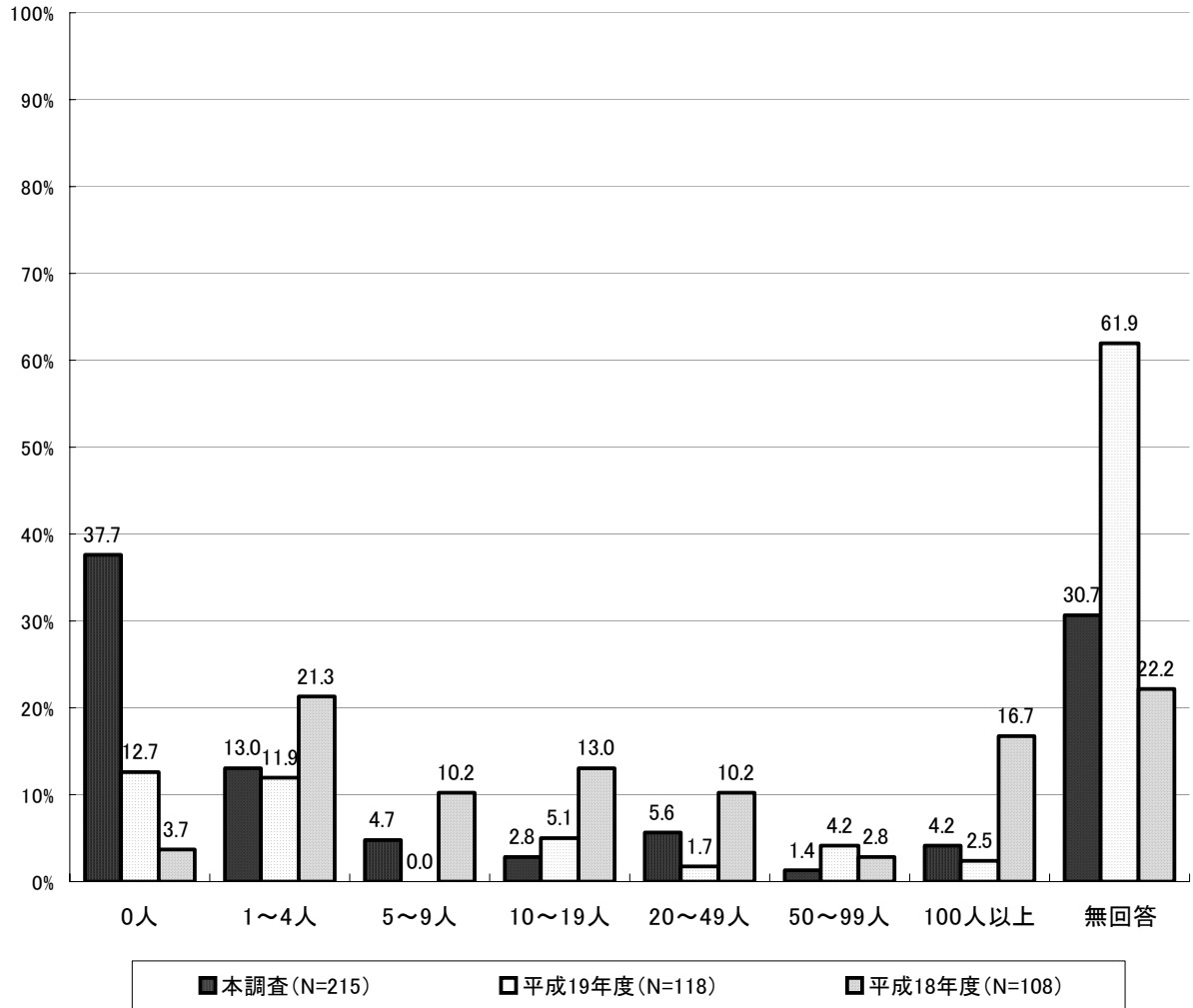
研究開発人員をみると、企業では「1～4人」「5～9人」がそれぞれ5.9%（6件）、大学では「1～4人」が19.5%（22件）で最も多くなっている。但し、「20～49人」が全体で5.6%（12件）、「100人以上」が4.2%（9件）となっており、中～大規模人員を抱えるところも数は少ないながらも一定数確認できる。



【経年比較（全体）】

今回調査では開発人員「1～4人」が13.0%（28件）と小規模人員が主流となっている。

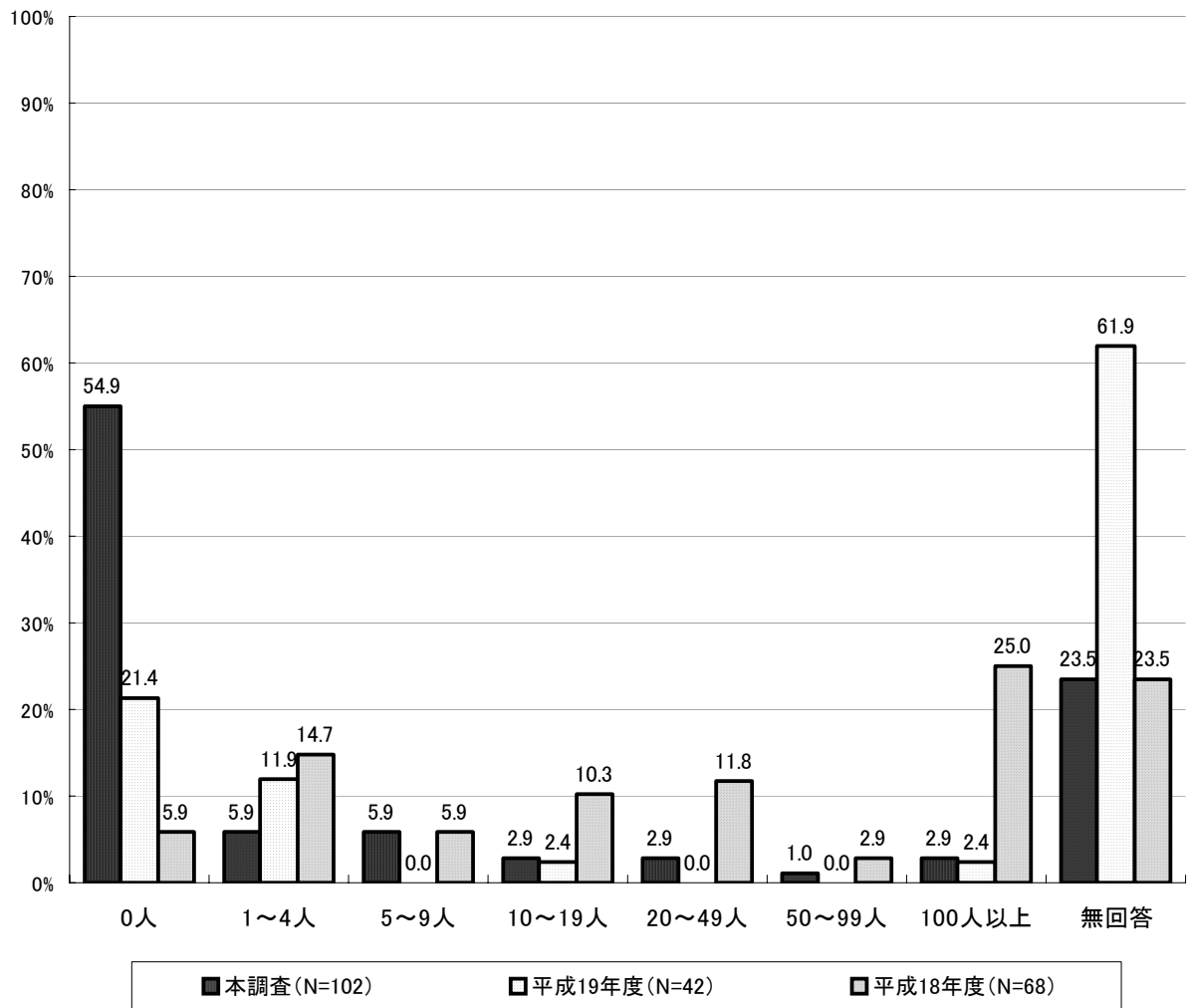
【経年比較（全体）】研究開発に携わっている人数(SA)



【経年比較（企業）】

企業では、開発人員「1～4人」「5～9人」がそれぞれ5.9%（6件）で最多となっている。有効回答数が少なく傾向は捉えにくいだが、昨年度以前と同様、比較的小規模な人員構成が主流と考えられる。

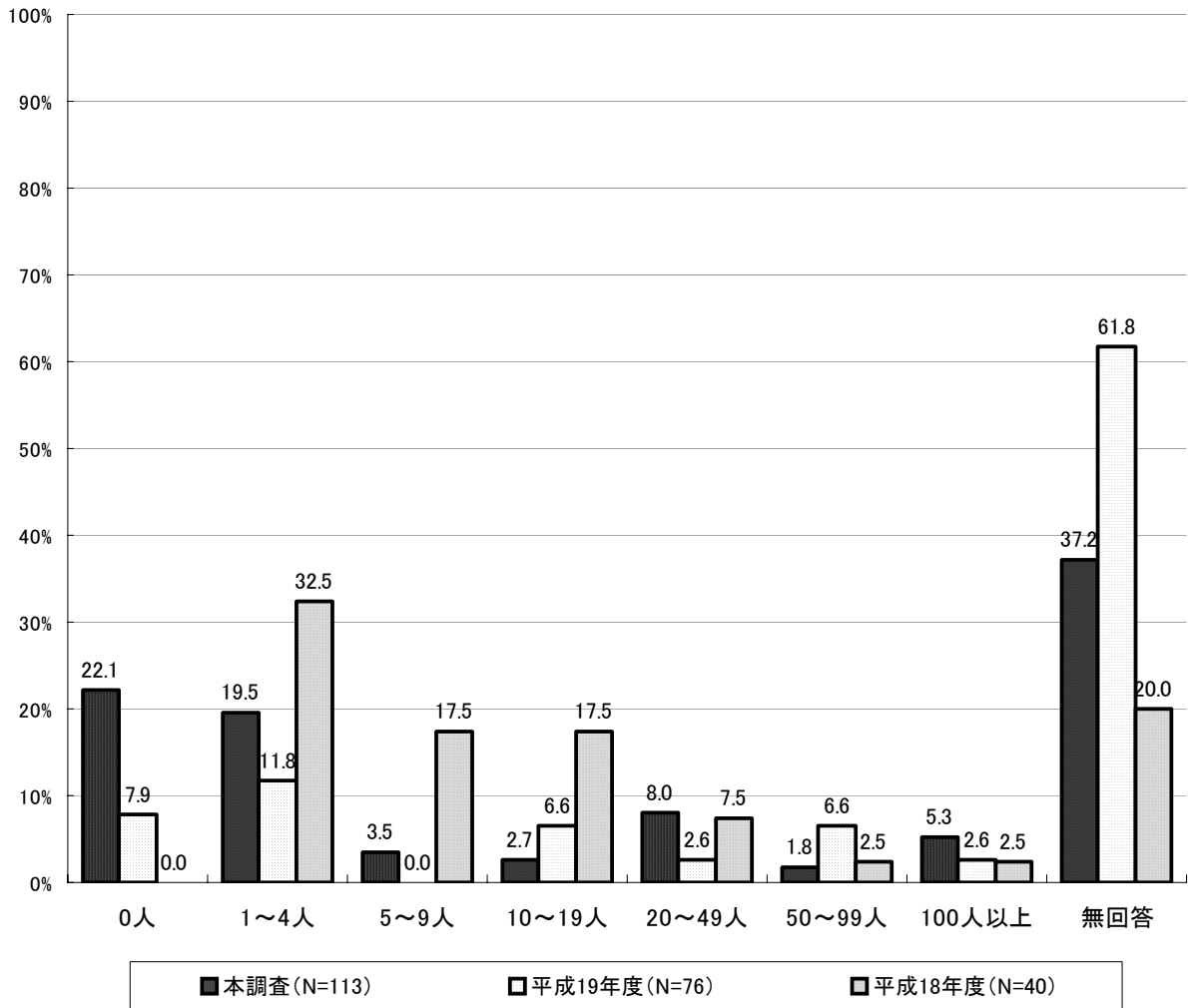
【経年比較（企業）】研究開発に携わっている人数(SA)



【経年比較（大学）】

今年度調査では、昨年度同様「1～4人」の19.5%（22件）が最多でかつ、増加傾向が見られる。但し、「20～49人」「100人以上」の割合もそれぞれ増加しており、一概に開発人員が減少しているとは捉えられない。

【経年比較(大学)】研究開発に携わっている人数(SA)



## (2) 年間の研究開発費

### 【本調査】

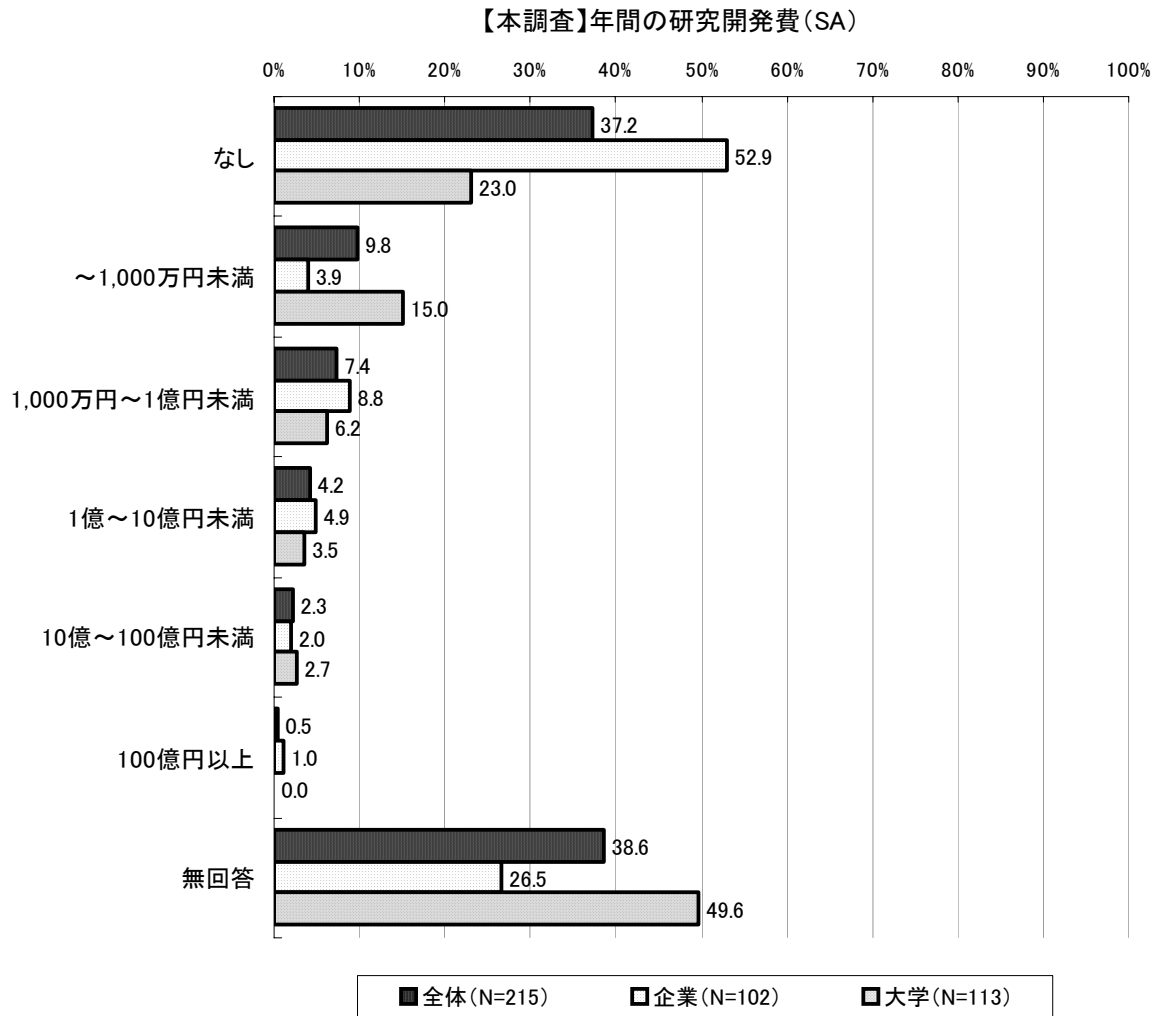
○年間研究開発費について、回答が得られた層をみていくと、1,000 万円未満から 1 億～10 億円未満を主として、幅広い層に分布していることが確認できる。

### 【経年比較】

○年間研究開発費が小規模のものから中～大規模開発に至るまで、一定数が確認でき、金額帯ごとの回答分布の傾向は昨年度と同様の傾向にあると言える。

【本調査】

全体ベースで見ると、「～1,000万円未満」が9.8%（21件）、「1,000万円～1億円未満」が7.4%（16件）、「1億～10億円未満」が4.2%（9件）と年間研究開発費は昨年度同様、比較的幅広く分布している。大学では「～1,000万円未満」が15.0%（17件）と、全体と比べて割合が高い傾向が見られる。

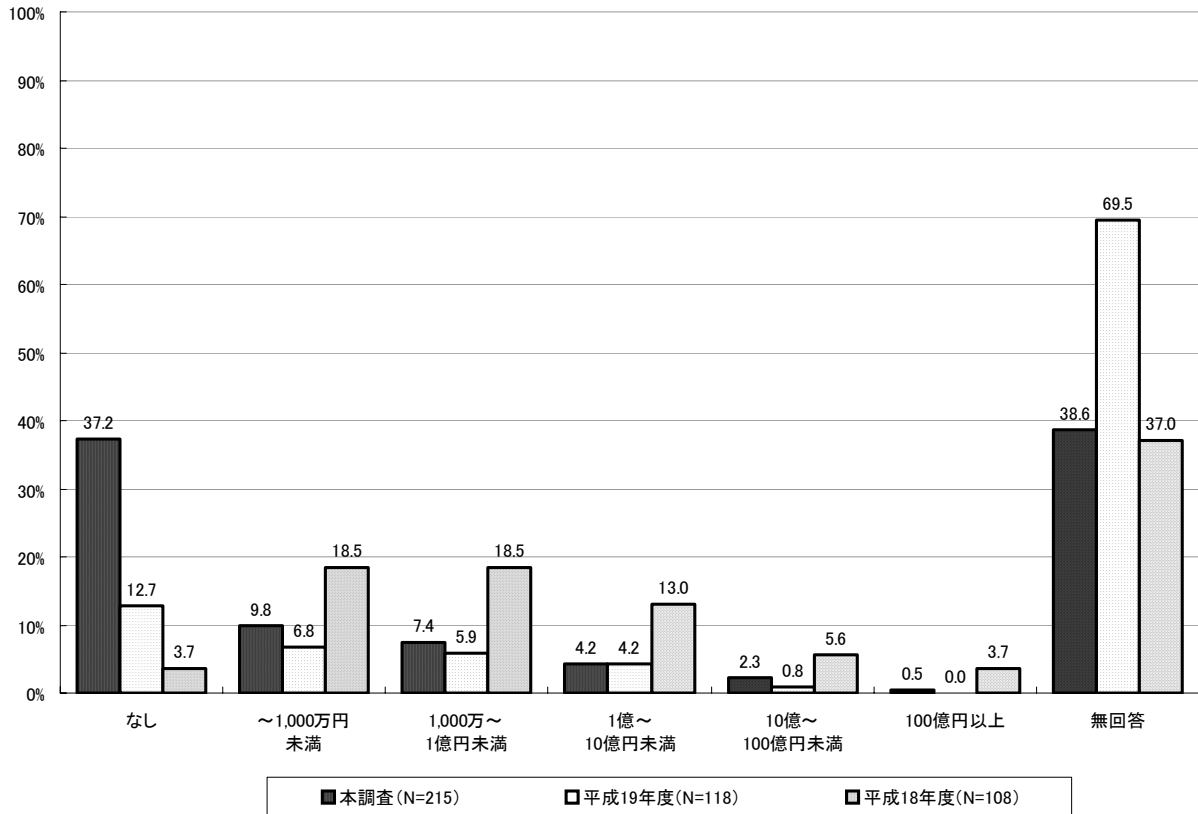


【経年比較（全体）】

全体では、「～1,000万円未満」が9.8%（21件）、「1,000万～1億円未満」が7.4%（16件）、「1億～10億円未満」が4.2%（9件）となっている。

年間研究開発費が小規模のものから中～大規模開発まで一定数確認でき、金額帯ごとの分布においても、昨年度と同様の傾向にあると言える。

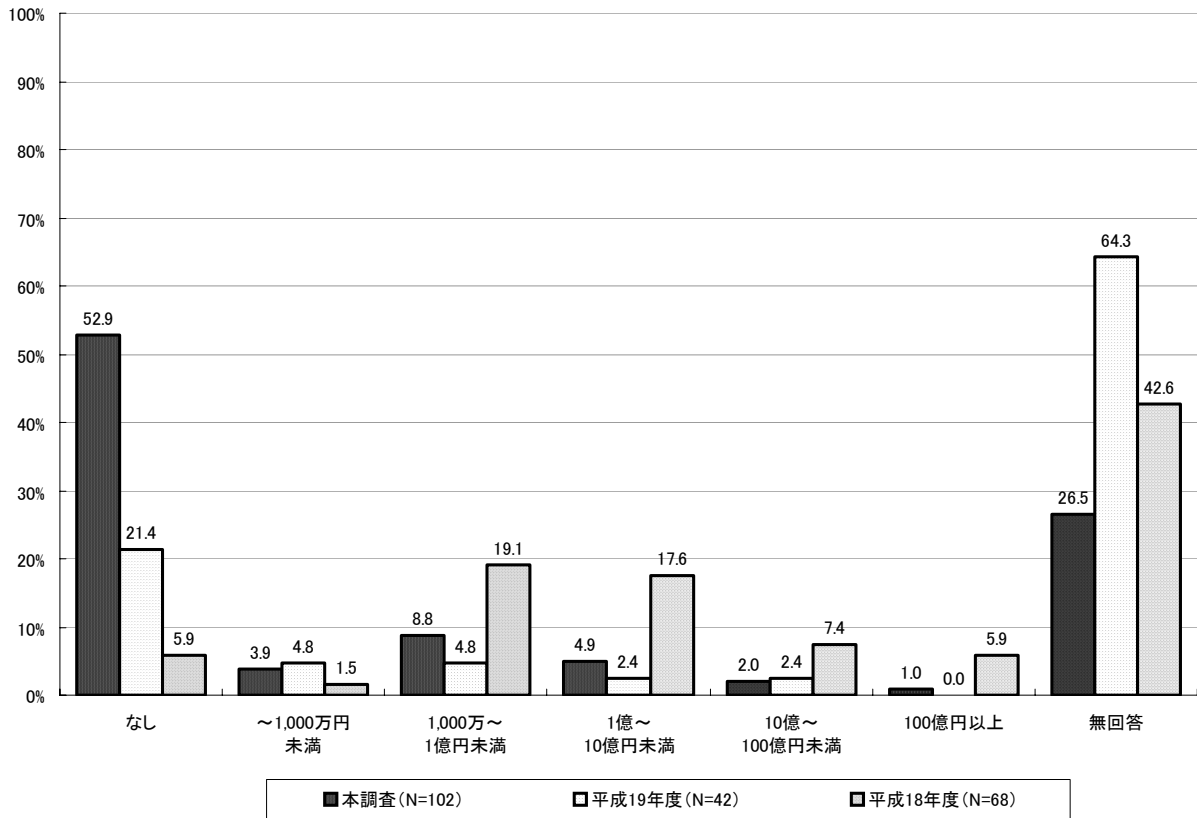
【経年比較（全体）】年間の研究開発費（SA）



【経年比較（企業）】

今年度は、「～1,000万円未満」が3.9%（4件）、「1,000万～1億円未満」が8.8%（9件）、「1億～10億円未満」が4.9%（5件）と、昨年度同様、有効回答数は少ないものの回答自体は幅広く分布している。

【経年比較（企業）】年間の研究開発費（SA）

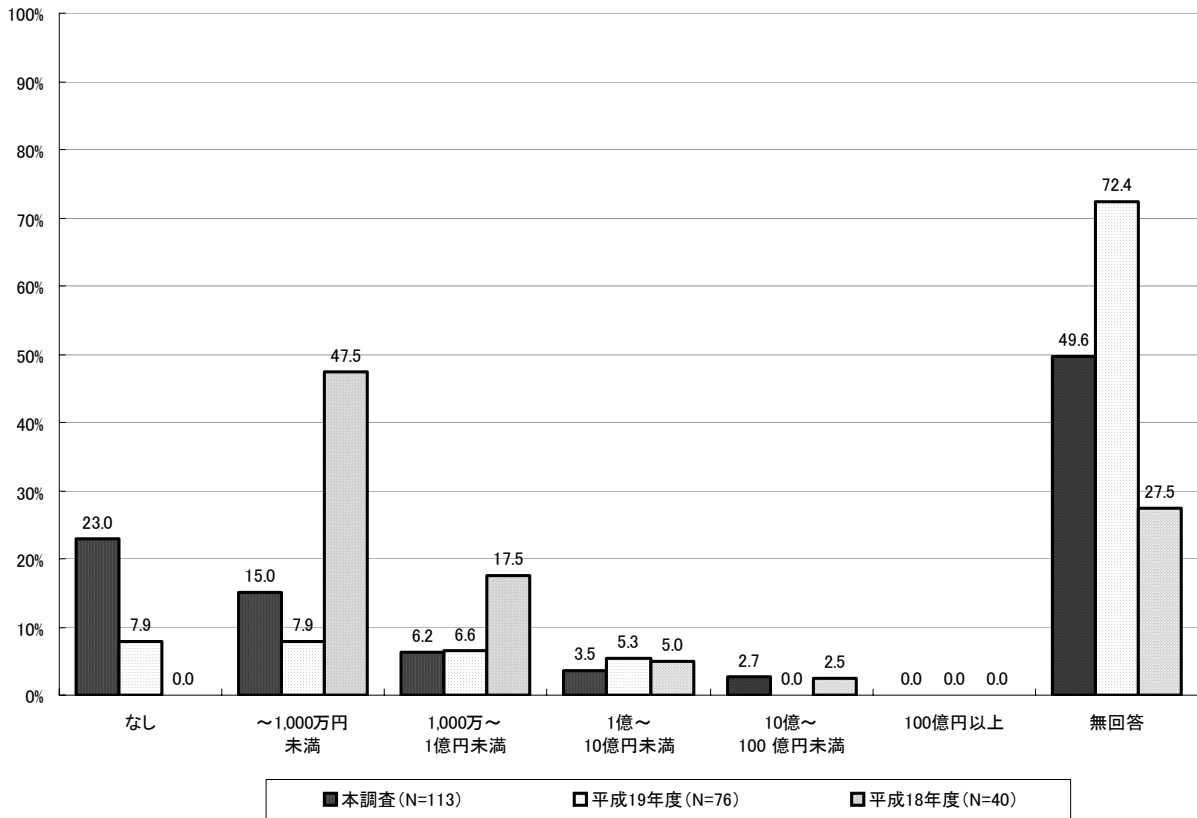




【経年比較（大学）】

今年度は、「～1,000万円未満」が15.0%（17件）、「1,000万～1億円未満」が6.2%（7件）、「1億～10億円未満」が3.5%（4件）と、昨年度同様、回答自体は小規模から中～大規模開発まで幅広く分布している。

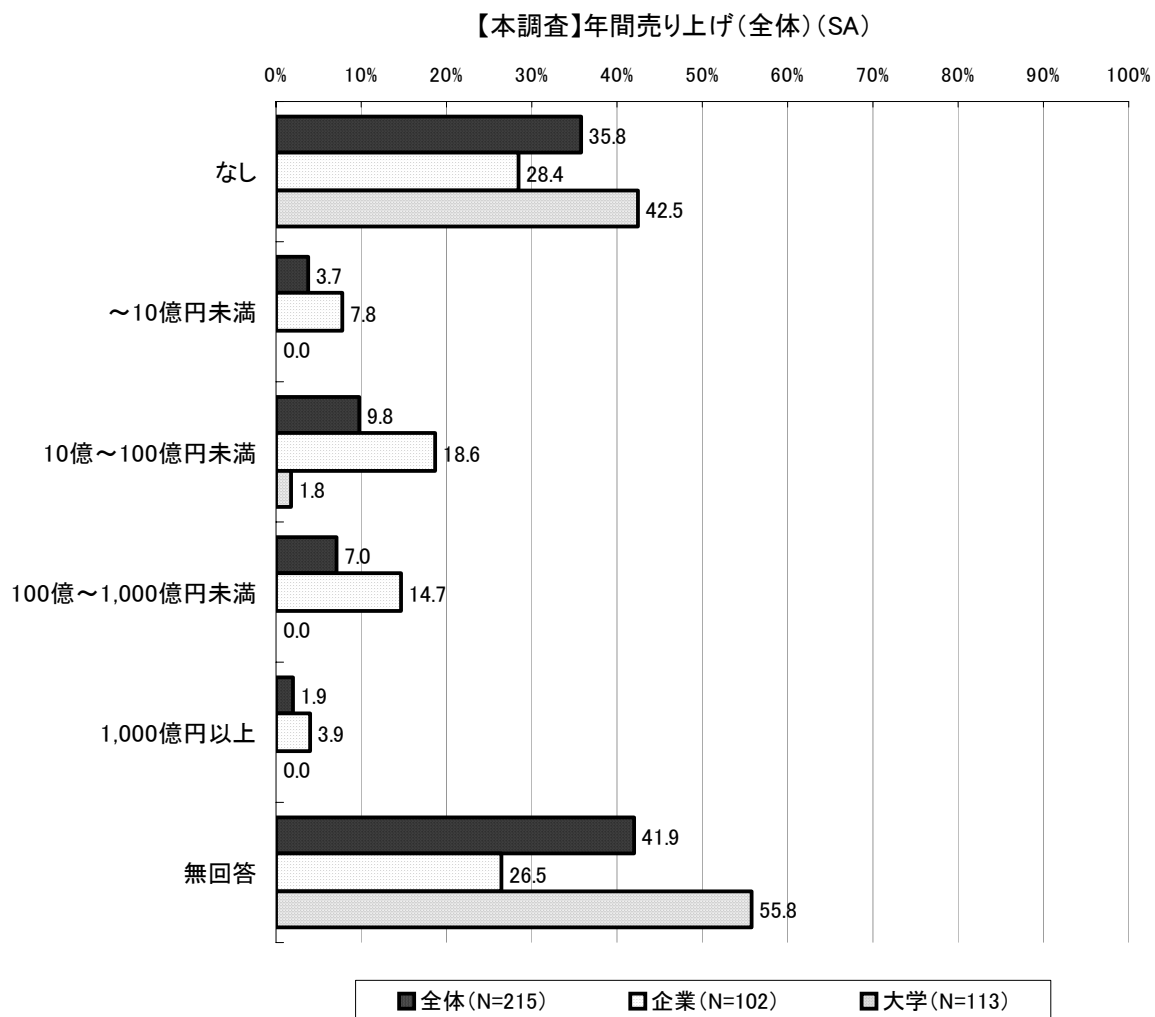
【経年比較（大学）】年間の研究開発費（SA）



### (3) 年間売り上げ（全体）

#### 【本調査】

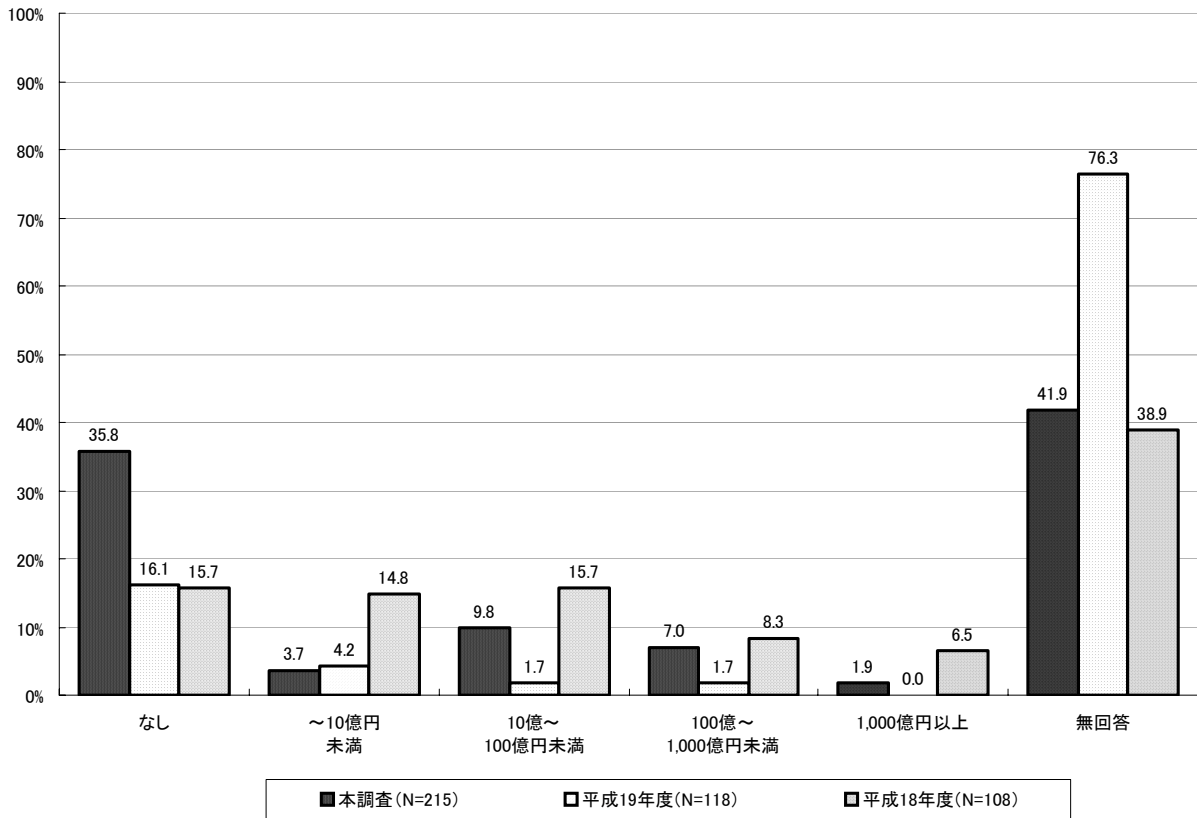
年間売り上げに関しては、「なし」が全体ベースでは35.8%（77件）で最多となり、その回答の大部分を「大学」が占めている。企業では、有効回答のうち「10億～100億円未満」の割合が最多で18.6%（19件）となっている。



【経年比較（全体）】

全体ベースでの有効回答のうち、最も多いのは売上高「10億～100億円未満」の9.8%（21件）で、次いで「100億～1,000億円未満」が7.0%（15件）と続いている。これらの開発費層は昨年度と比べて特に割合が高くなっていると言える。

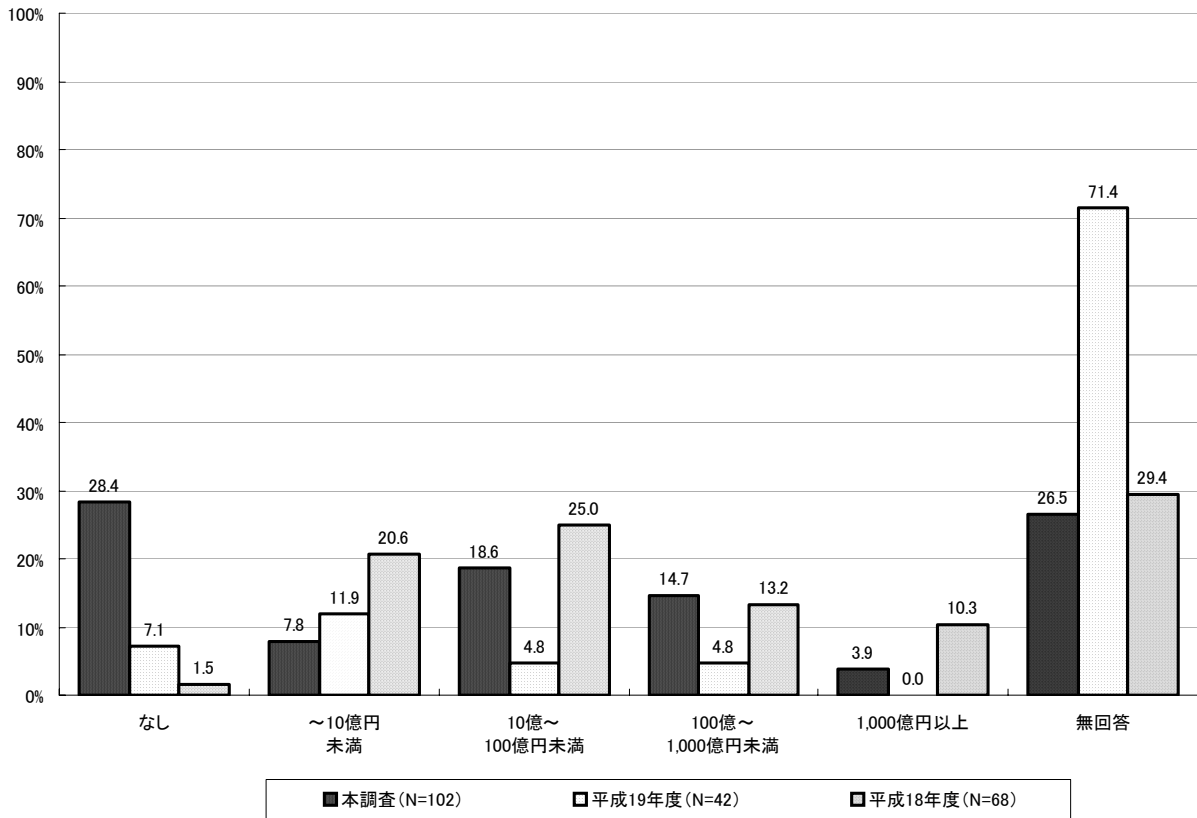
【経年比較（全体）】年間売り上げ（全体）（SA）



【経年比較（企業）】

企業では、有効回答のうち「10億～100億円未満」が18.6%（19件）と最も高く、次いで「100億～1,000億円未満」が14.7%（15件）と続く。これらの層は昨年度に比べ割合が増えており、一方で「～10億円未満」の層は昨年度よりも減少している。

【経年比較（企業）】年間売り上げ(全体)(SA)

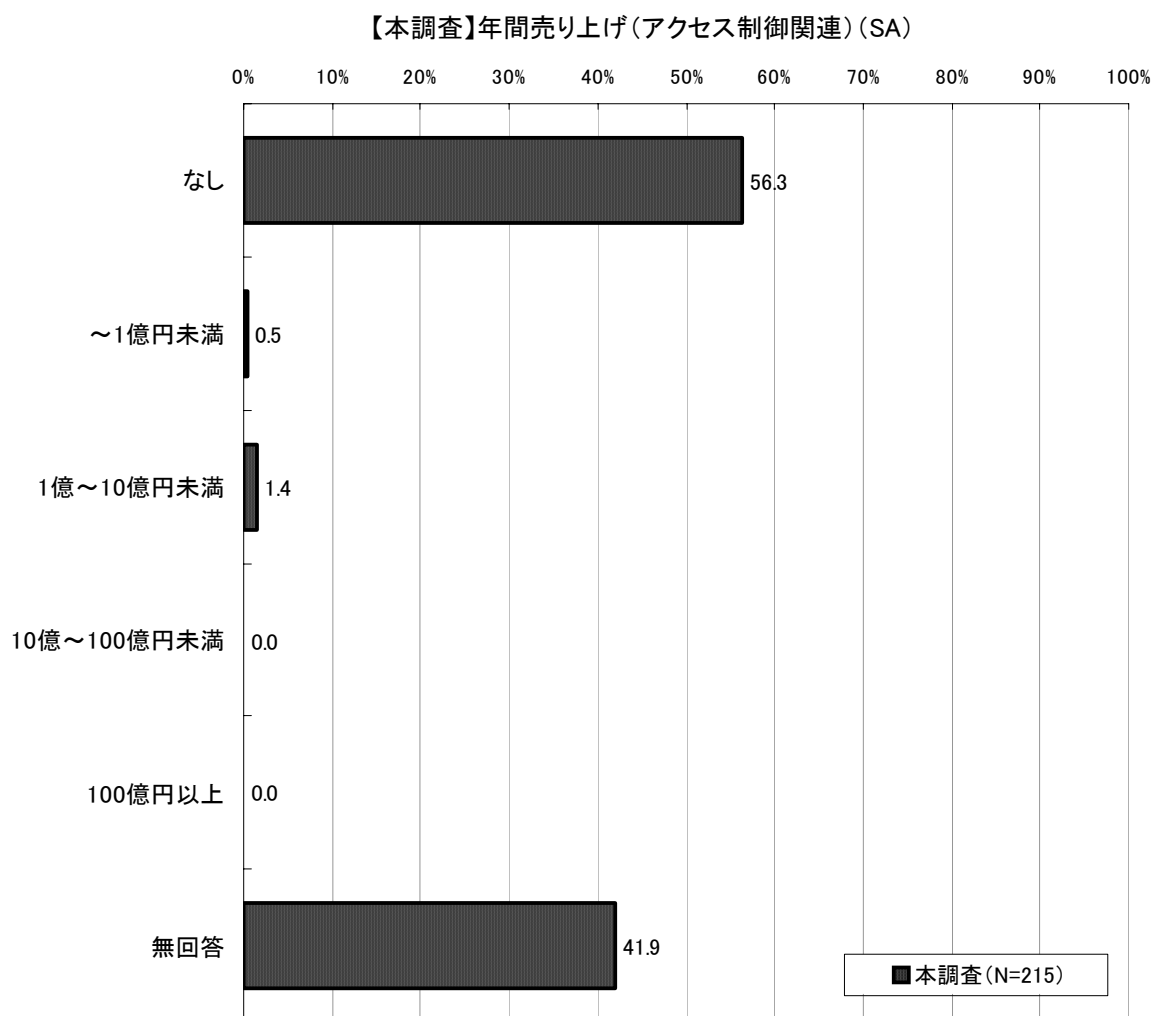


#### (4) 年間売り上げ（アクセス制御関連）

##### 【本調査】

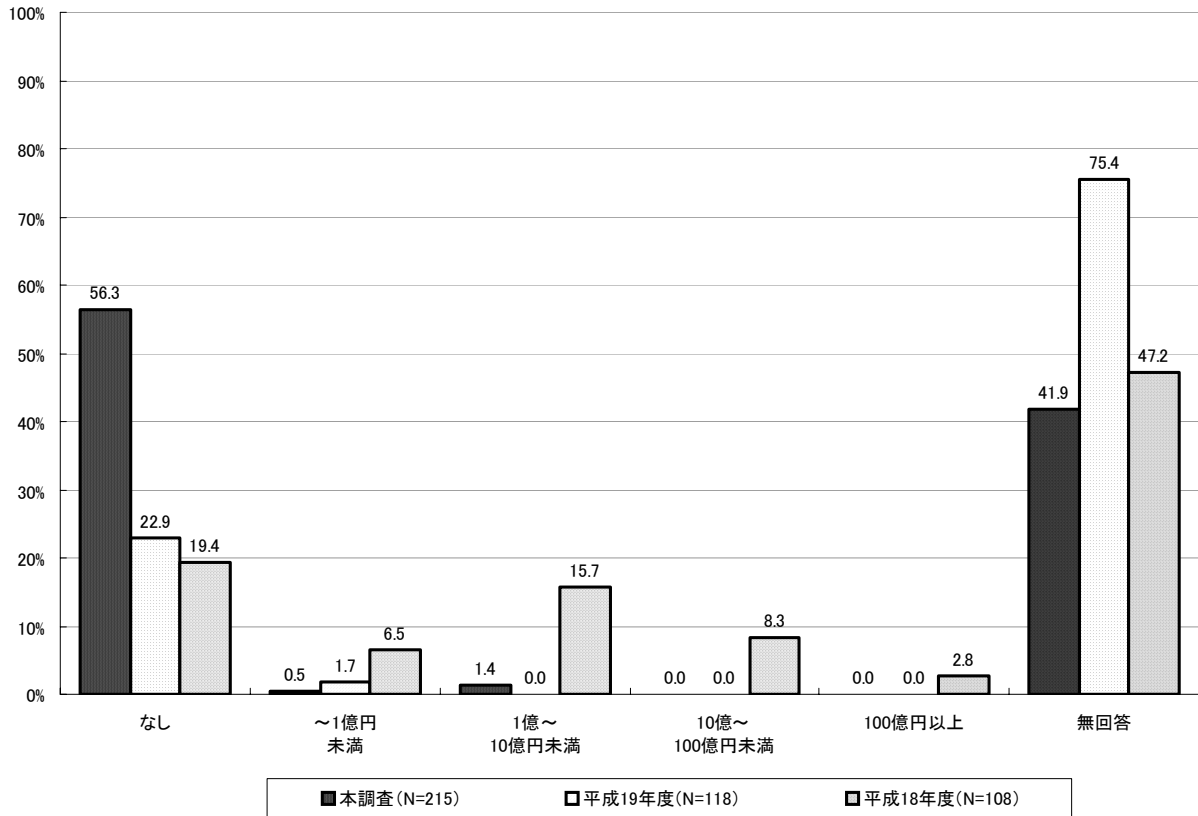
アクセス制御関連で売り上げがあったのは、「～1億円未満」で0.5%（1件）、「1億～10億円未満」で1.4%（3件）のみの回答となった。

売り上げ「なし」は56.3%（121件）となっており、その内訳は、企業68件、大学53件となる。

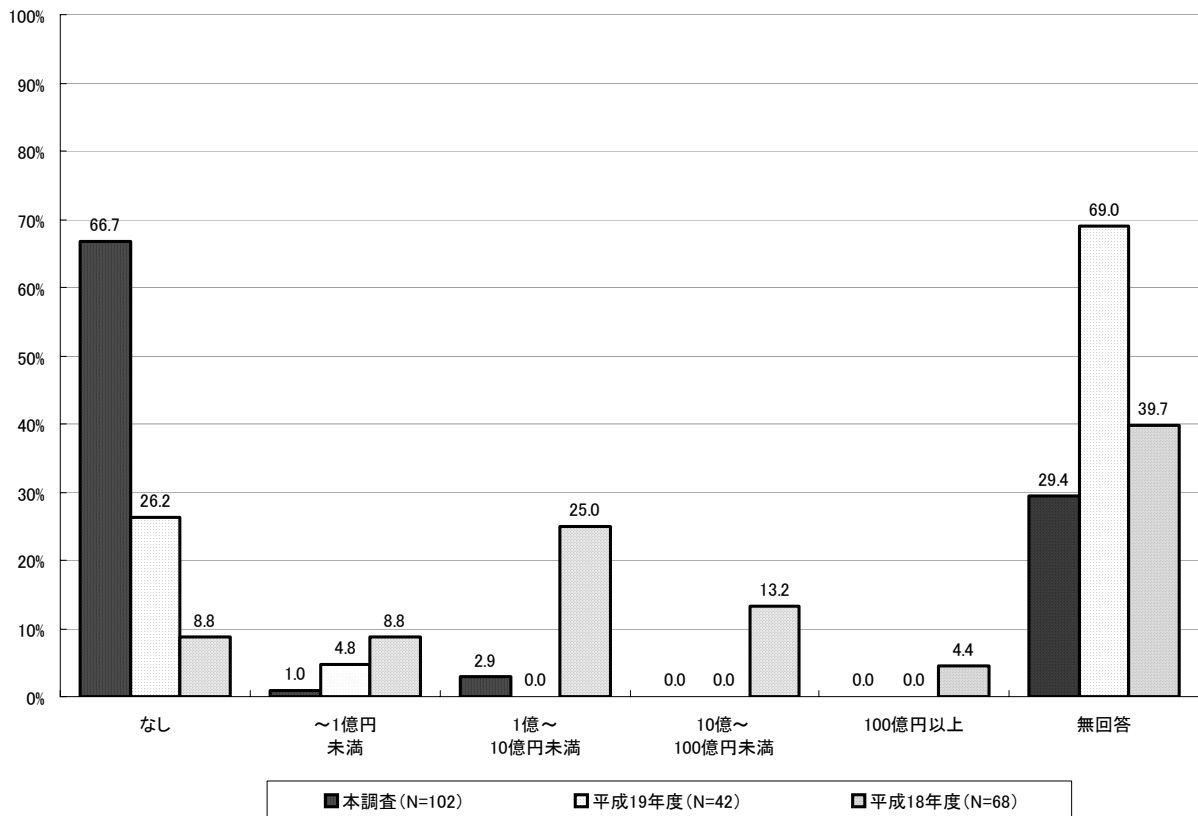


今年度は有効回答が非常に少なかったため、経年比較については、コメントを割愛した。

【経年比較(全体)】年間売り上げ(アクセス制御関連)(SA)



【経年比較(企業)】年間売り上げ(アクセス制御関連)(SA)



## 1.2 現在、取り組んでいる分野

### 【本調査】

- 企業、大学ともに「ネットワークセキュリティ」が最多となっている。  
次いで企業では「ウイルス対策」「認証技術」「不正侵入対策」、大学では「認証技術」「暗号技術」「不正侵入対策」が続く。

### 【経年比較】

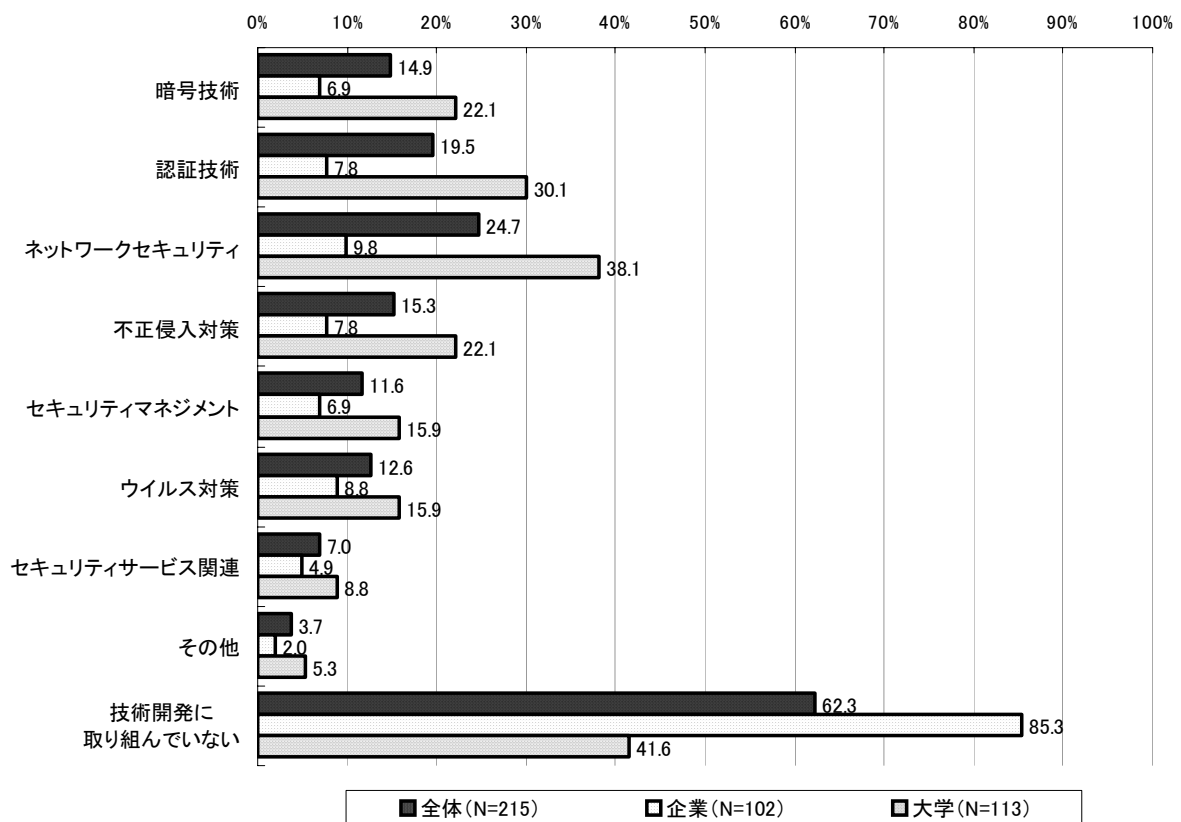
- 企業、大学ともに、昨年度と同様「ネットワークセキュリティ」が最多となっている。また「認証技術」「暗号技術」「セキュリティマネジメント」「ウイルス対策」の各項目は企業、大学のどちらにおいても昨年度と比べて割合は増加している。

【本調査】

企業においては、「ネットワークセキュリティ」が 9.8%（10 件）と最も高く、次いで「ウイルス対策」が 8.8%（9 件）、「認証技術」「不正侵入対策」が共に 7.8%（8 件）と続く。

大学においても企業と同様に、「ネットワークセキュリティ」が最多で 38.1%（43 件）となっている。次いで「認証技術」が 30.1%（34 件）、「暗号技術」「不正侵入対策」が共に 22.1%（25 件）と続く。

【本調査】現在、取り組んでいる分野(MA)

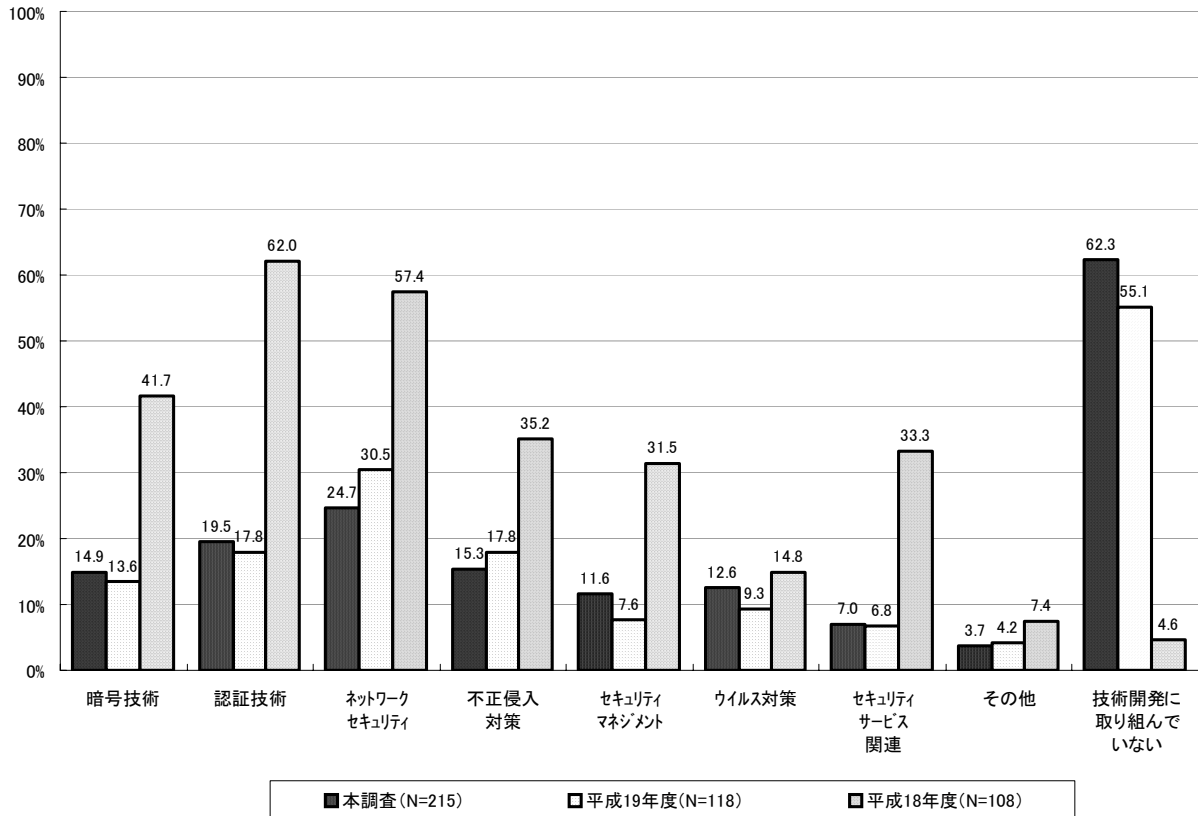




【経年比較（全体）】

「ネットワークセキュリティ」が 24.7%（53 件）で、昨年度と同様に最上位となっている。昨年度は「認証技術」「不正侵入対策」が共に 2 位であったが、今年度も「認証技術」が 19.5%（42 件）で 2 位、「不正侵入対策」が 15.3%（33 件）で 3 位となっており、全体的な傾向は昨年度から大きな変化は見られないと言える。

【経年比較(全体)】現在、取り組んでいる分野(MA)

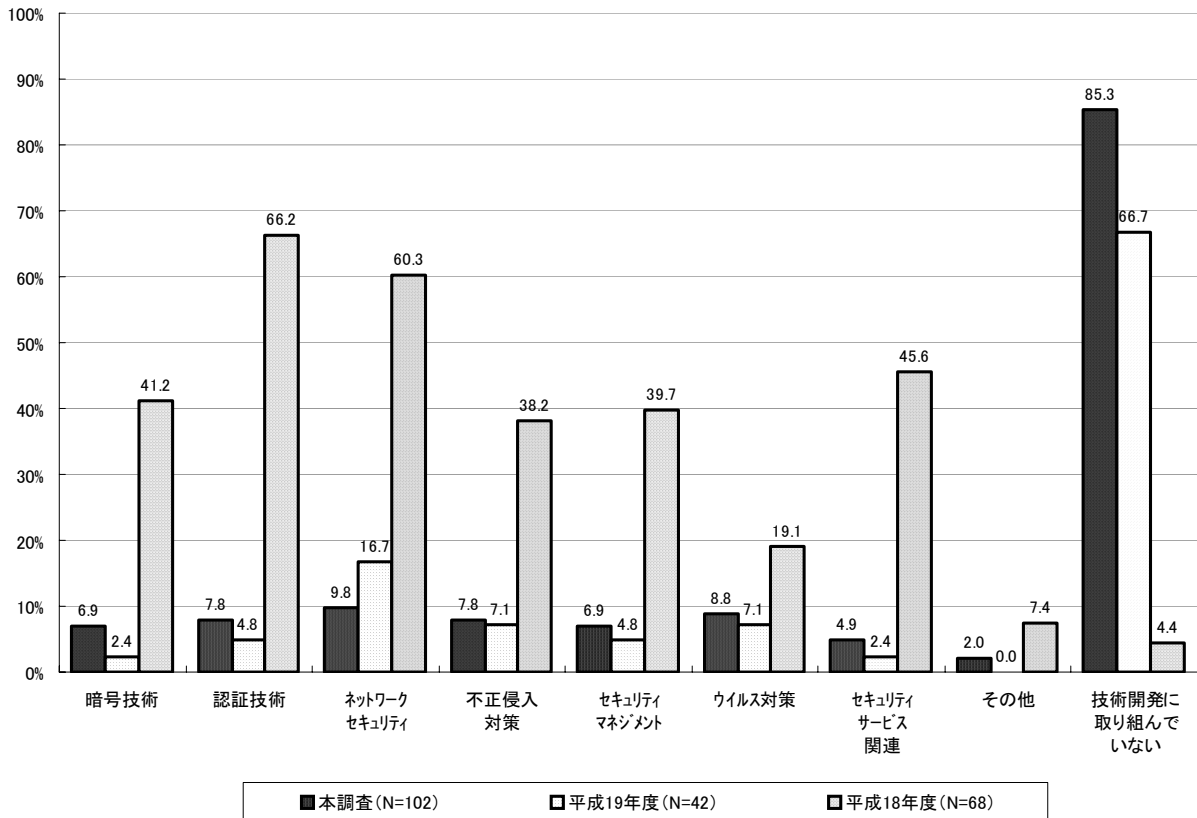


【経年比較（企業）】

企業についてみると、「ネットワークセキュリティ」が 9.8%（10 件）で、昨年度と同様に最上位となっている。昨年度、上位であった「ウイルス対策」「不正侵入対策」はそれぞれ、今年度も「ウイルス対策」が 8.8%（9 件）で 2 位、「不正侵入対策」が「認証技術」とともに 7.8%（8 件）で 3 位となっている。

また、「暗号技術」は、6.9%（7 件）となっており、昨年度と比べて割合が増加していることが確認できる。

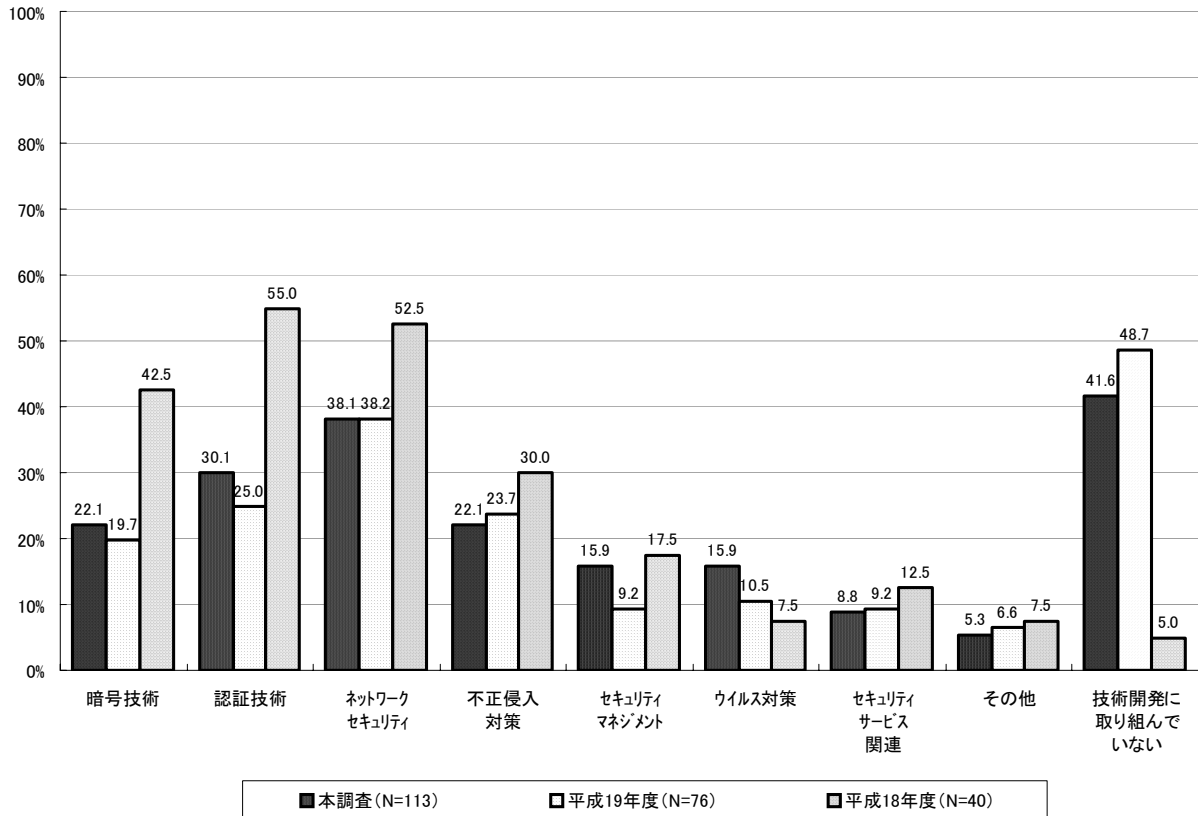
【経年比較（企業）】現在、取り組んでいる分野(MA)



【経年比較（大学）】

大学についてみると、「ネットワークセキュリティ」が38.1%（43件）で、昨年度と同様に最上位となっている。昨年度、上位であった「認証技術」「不正侵入対策」はそれぞれ、今年度も「認証技術」が30.1%（34件）で2位、「不正侵入対策」が「暗号技術」とともに22.1%（25件）で3位となっている。

【経年比較(大学)】現在、取り組んでいる分野(MA)



### 1.3 今後、取り組んでいく分野

#### 【本調査】

○今後の取り組み分野をみると、企業からの回答は比較的幅広いのに対し、大学では「ネットワークセキュリティ」を最多に、「認証技術」「セキュリティマネジメント」等の分野に回答が集まっている傾向にある。

#### 【経年比較】

○全体ベースでみると、「ネットワークセキュリティ」を最多に、「認証技術」が続いており、昨年度と同様の傾向と言える。

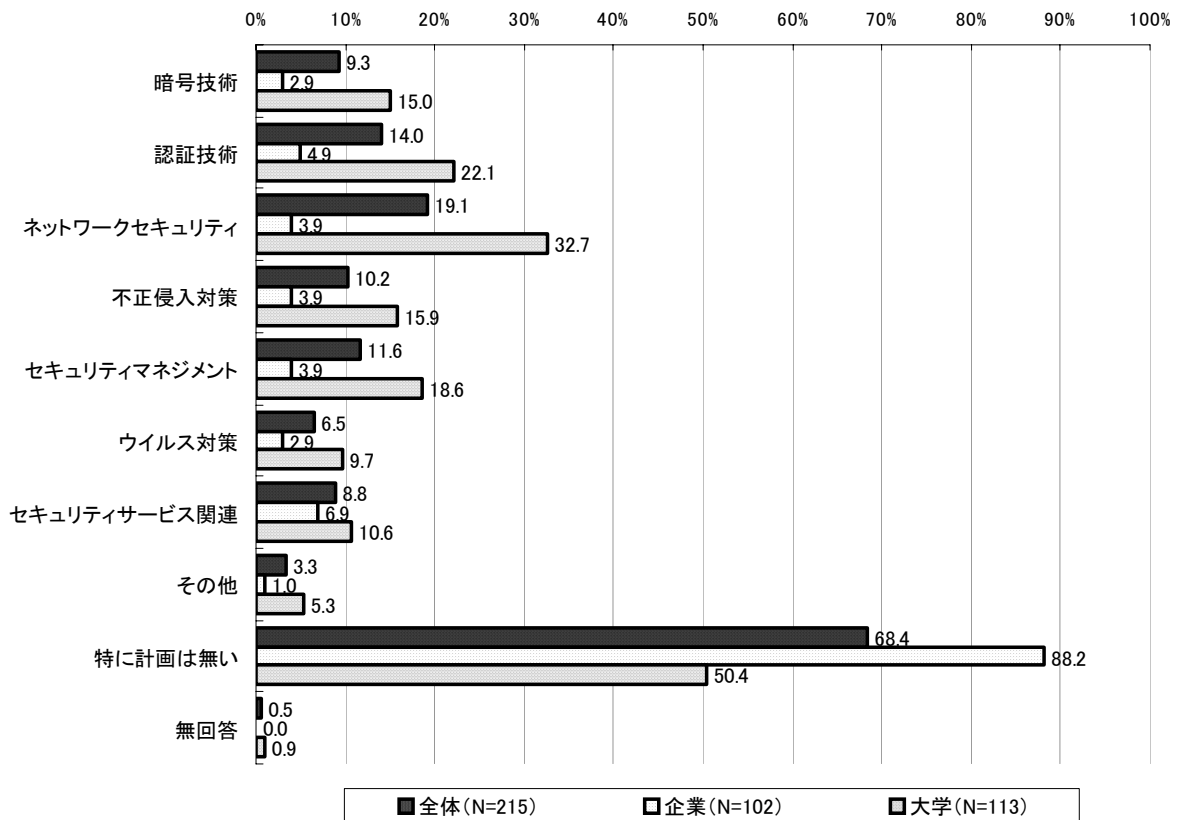
○大学においても「ネットワークセキュリティ」「認証技術」の上位分野に変化はないものの、「セキュリティマネジメント」が昨年度に比べて相対的に割合が高まり、上位分野となっている。

【本調査】

今後取り組んでいく分野は、企業では各分野とも、それぞれ 3～7%（3～7 件）程度の間比較的幅広く分布している。

一方、大学では「ネットワークセキュリティ」の 32.7%（37 件）を最多として、「認証技術」の 22.1%（25 件）などが特に割合が高くなっており、企業と大学では取り組み予定分野の傾向は異なっている。

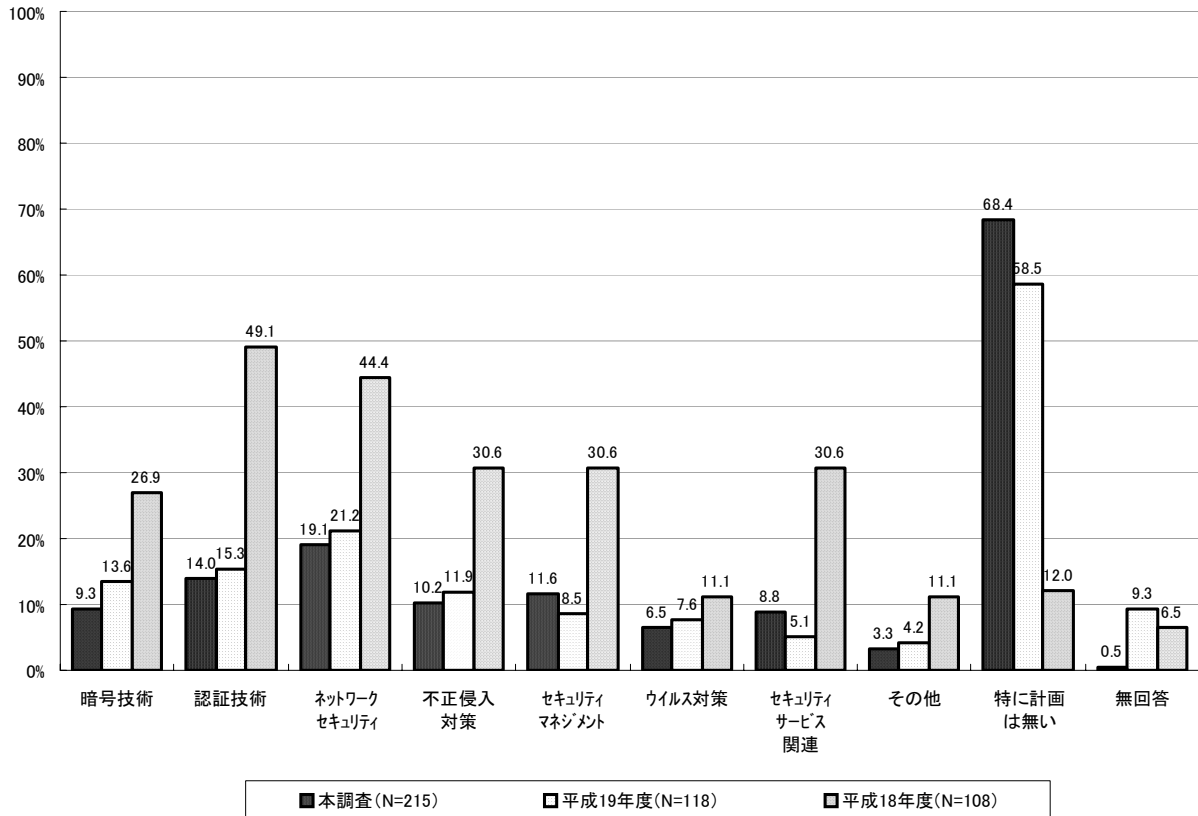
【本調査】今後、取り組んでいく分野(MA)



【経年比較（全体）】

全体で見ると、「ネットワークセキュリティ」が最も割合が高く 19.1%（41 件）、次いで「認証技術」が 14.0%（30 件）、「セキュリティマネジメント」が 11.6%（25 件）と続いており、特に上位 2 分野の順位は昨年度と変化がなく、全体的にも昨年度と同様の傾向となっている。

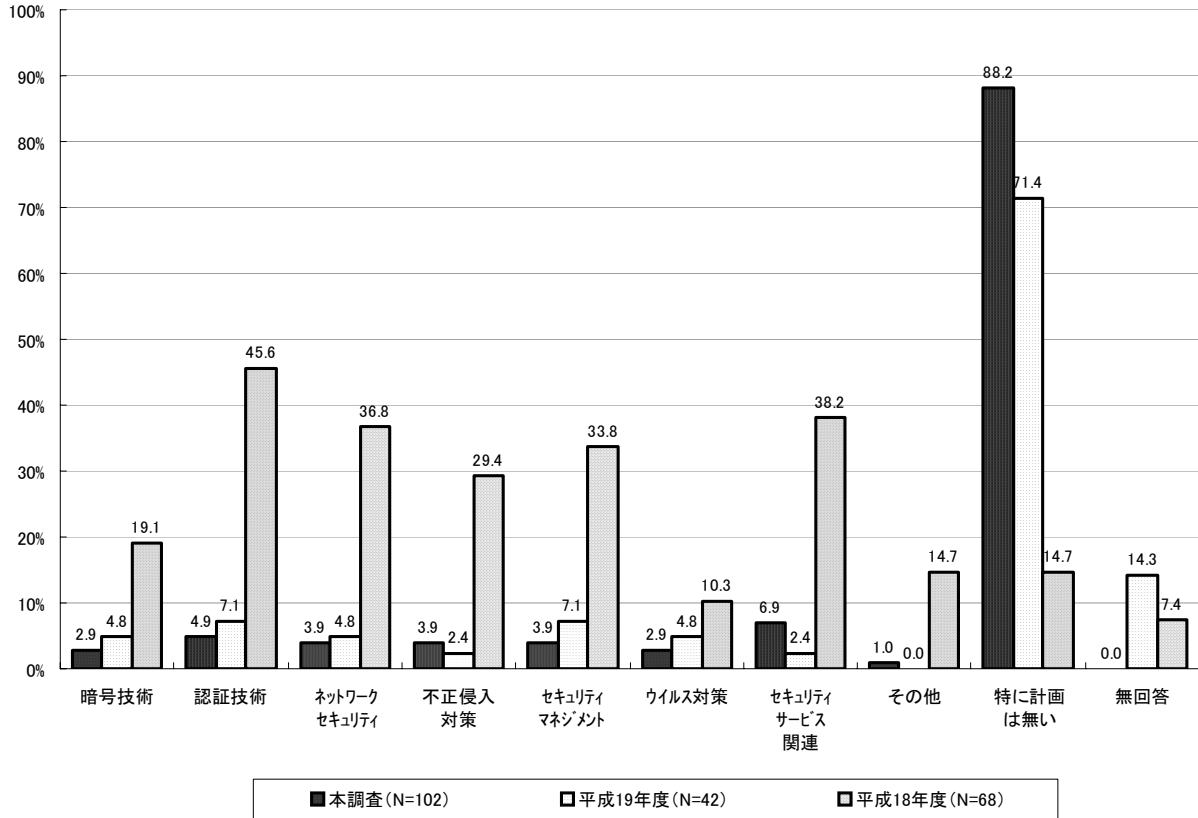
【経年比較（全体）】今後、取り組んでいく分野(MA)



【経年比較（企業）】

昨年度と同様、各分野に回答が幅広く分布しているが、「セキュリティサービス関連」が6.9%（7件）と昨年度よりも割合が特に高まっている。

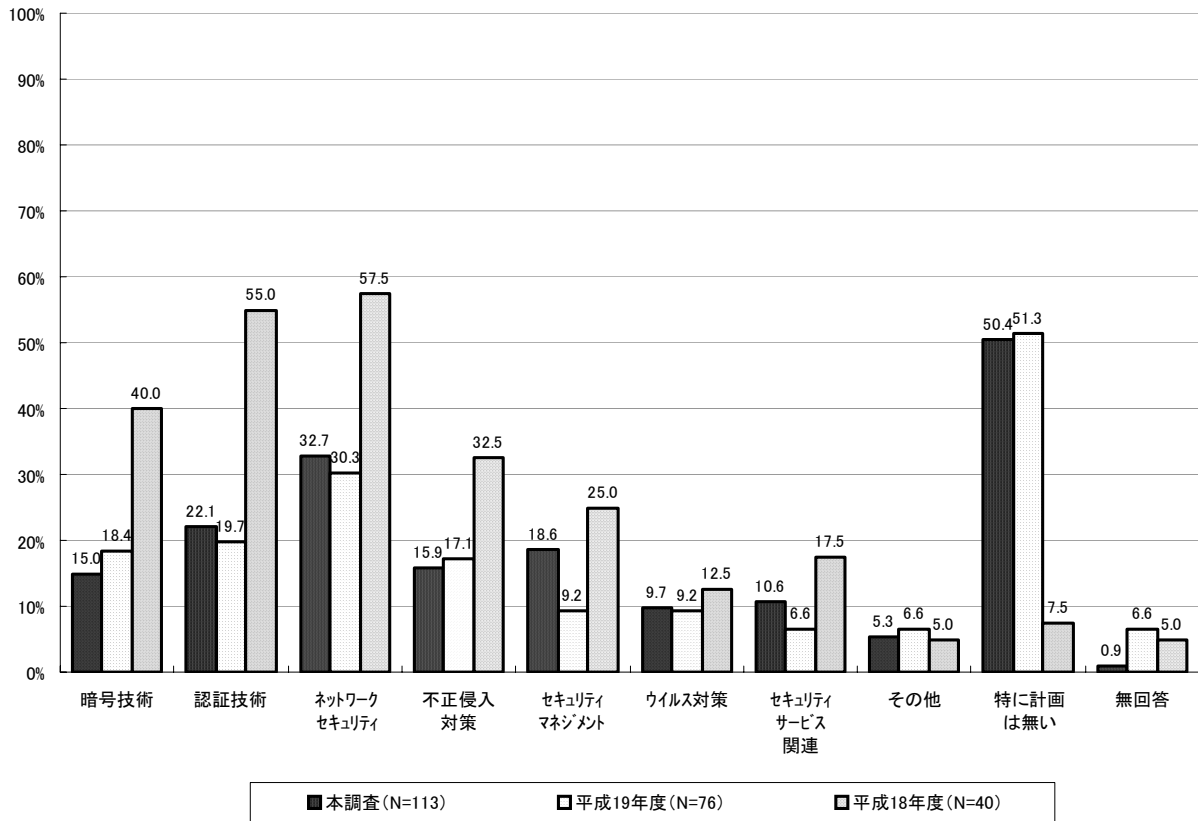
【経年比較（企業）】今後、取り組んでいく分野（MA）



【経年比較（大学）】

「ネットワークセキュリティ」が32.7%（37件）、「認証技術」が22.1%（25件）と上位2分野の順位は変わらないものの、「セキュリティマネジメント」が18.6%（21件）で3位となっており、昨年度に比べて相対的に割合が高くなっている。

【経年比較(大学)】今後、取り組んでいく分野(MA)





## 1.4 今後、最も力を入れていく分野

### 【本調査】

- 企業からの回答が少なく傾向を捉えにくいですが、大学においては「ネットワークセキュリティ」の割合が非常に高くなっている。

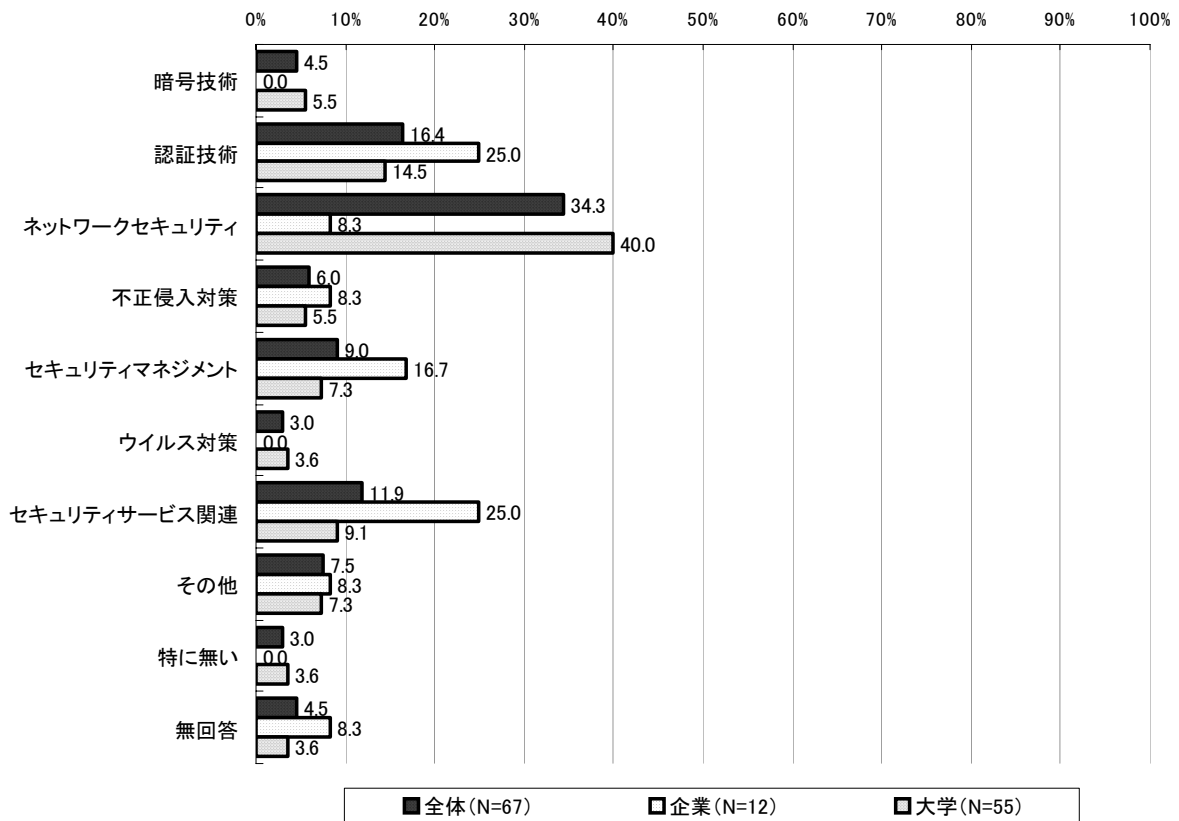
### 【経年比較】

- 昨年度と同様、「ネットワークセキュリティ」が今後、最も力を入れていく分野として挙げられている。
- 「セキュリティサービス関連」が昨年度と比べ割合が大きくなっている一方で、昨年度の上位分野であった「暗号技術」は大きく割合を下げている。

【本調査】

企業については、各分野への回答が1～3件と少ないため、傾向を捉えることが難しい。  
 大学については、「ネットワークセキュリティ」の割合が非常に高く、40.0%（22件）  
 となっている。次いで「認証技術」の14.5%（8件）、「セキュリティサービス関連」の9.1%  
 （5件）と続く。

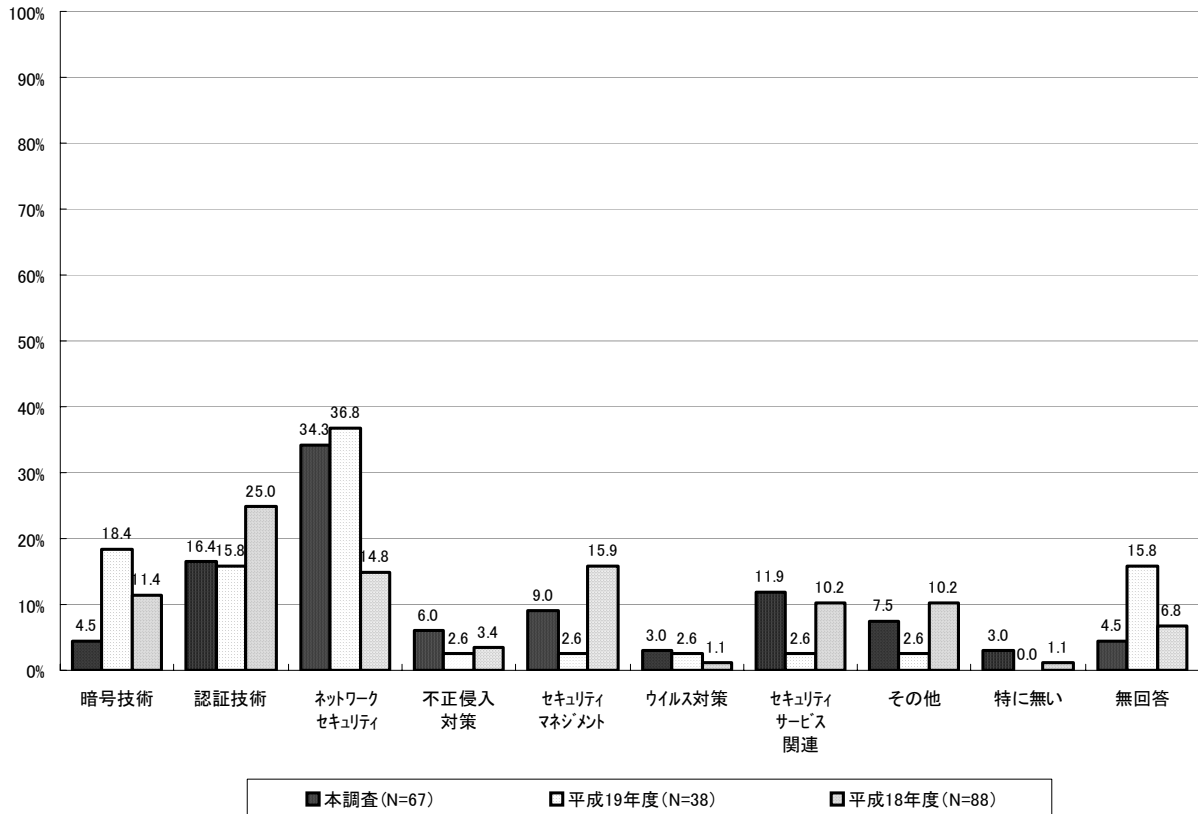
【本調査】今後、最も力を入れていく分野(SA)



【経年比較（全体）】

「ネットワークセキュリティ」が 34.3%（23 件）で最多となっており、次いで「認証技術」が 16.4%（11 件）、「セキュリティサービス関連」が 11.9%（8 件）が続いている。「セキュリティサービス関連」が昨年度と比べて相対的に割合が高くなっている一方で、「暗号技術」は昨年度と比べ、大きく割合を下げている。

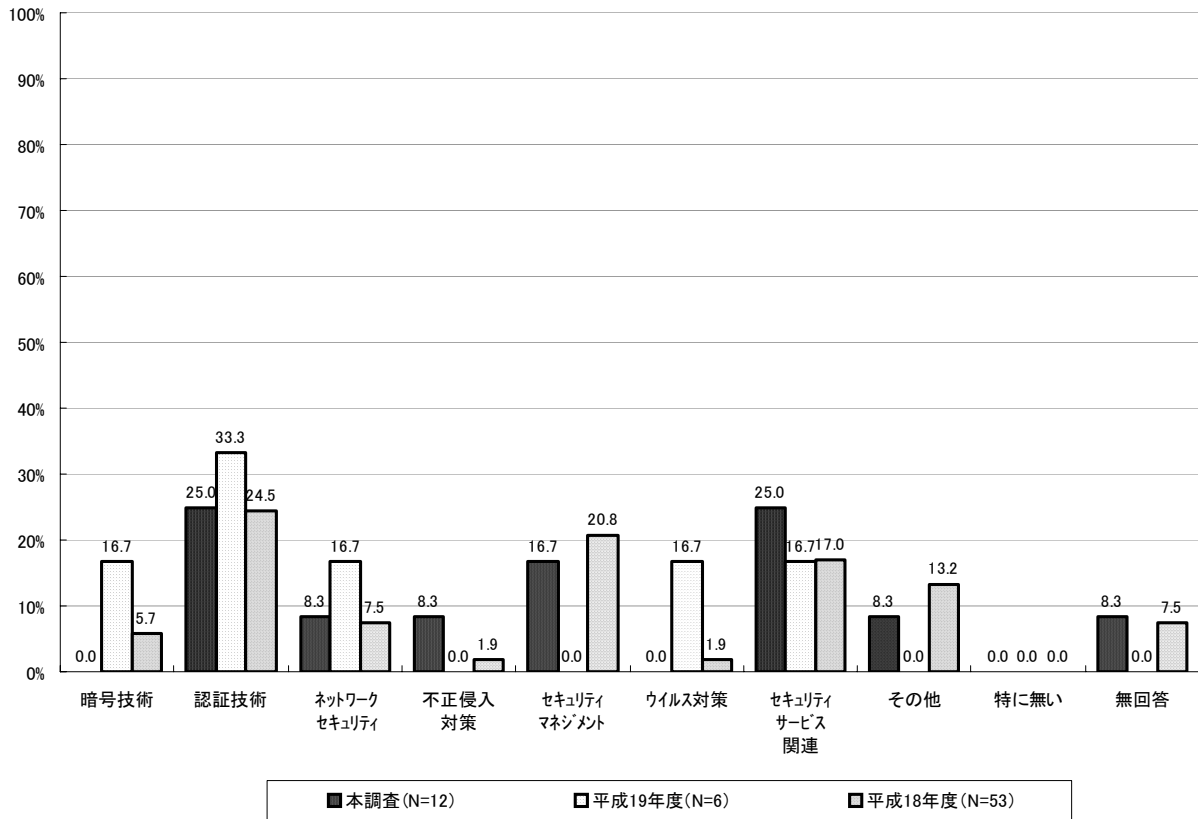
【経年比較（全体）】今後、最も力を入れていく分野(SA)



【経年比較（企業）】

企業については、各分野への回答が 1～3 件と少ないため、傾向を捉えることはできない。

【経年比較（企業）】今後、最も力を入れていく分野(SA)

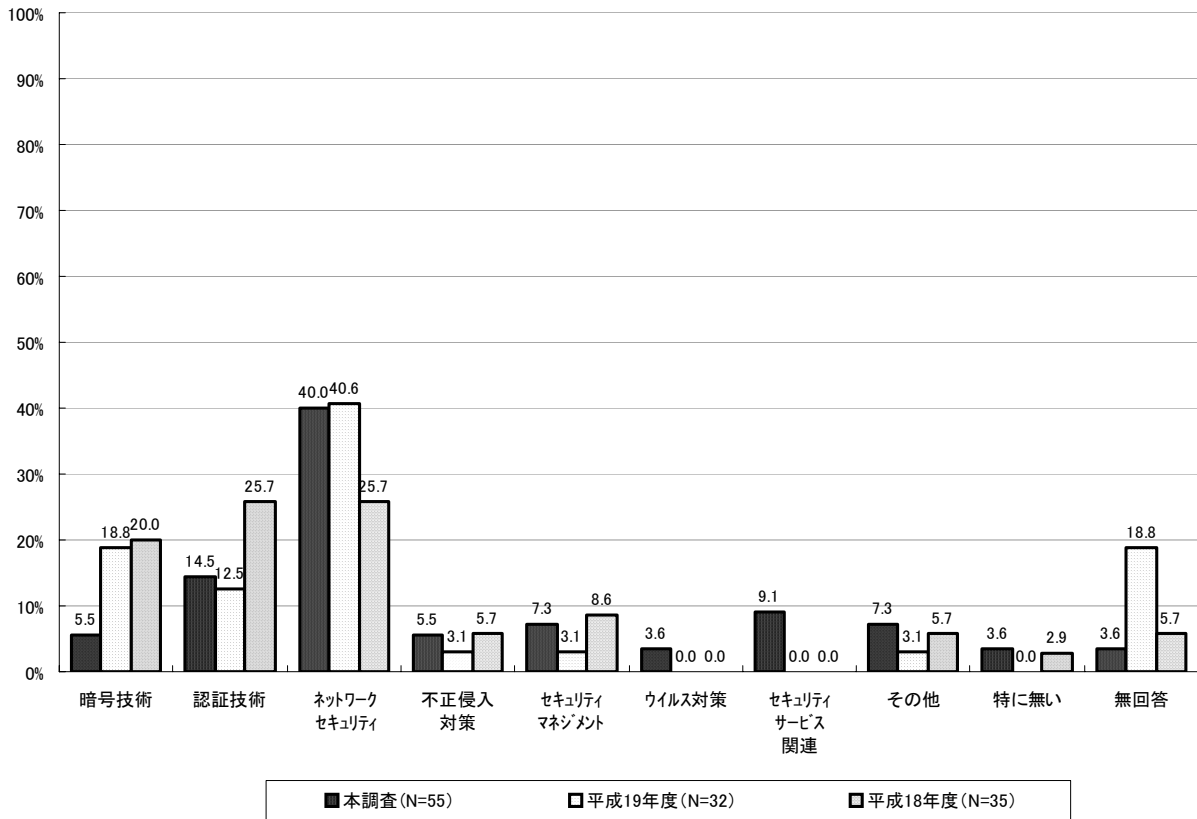


【経年比較（大学）】

今年度も昨年度と同様、「ネットワークセキュリティ」の割合が最も高く、40.0%（22件）を占めている。

昨年、一昨年ともに回答が見られなかった「セキュリティサービス関連」が9.1%（5件）と相対的に割合を高めており、今後、最も力を入れていく研究分野として捉えられつつあることがうかがえる。

【経年比較(大学)】今後、最も力を入れていく分野(SA)



## 1.5 現在、実用化（製品化）されているアクセス制御機能

### 【本調査】

- 全体ベースで見ると、回答の多い順に「認証技術」「ネットワークセキュリティ」「ウイルス対策」となっている。

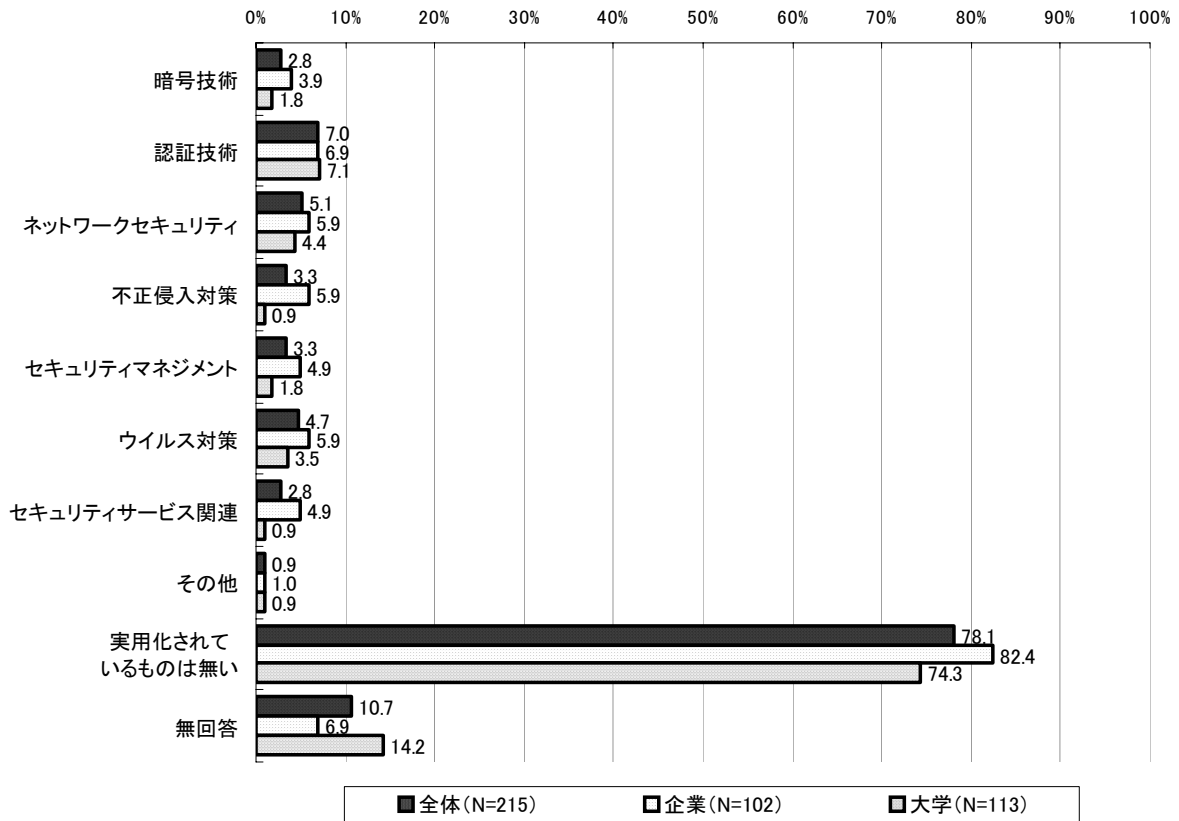
### 【経年比較】

- 昨年度の上位分野であった「認証技術」「ネットワークセキュリティ」が今年度においても上位2位を占めている。企業・大学の別にみても、「認証技術」が最上位、「ネットワークセキュリティ」がそれに続いている。

【本調査】

全体ベースでの分野別の内訳をみると、「認証技術」が 7.0%（15 件）、「ネットワークセキュリティ」が 5.1%（11 件）、「ウイルス対策」が 4.7%（10 件）の順となっている。

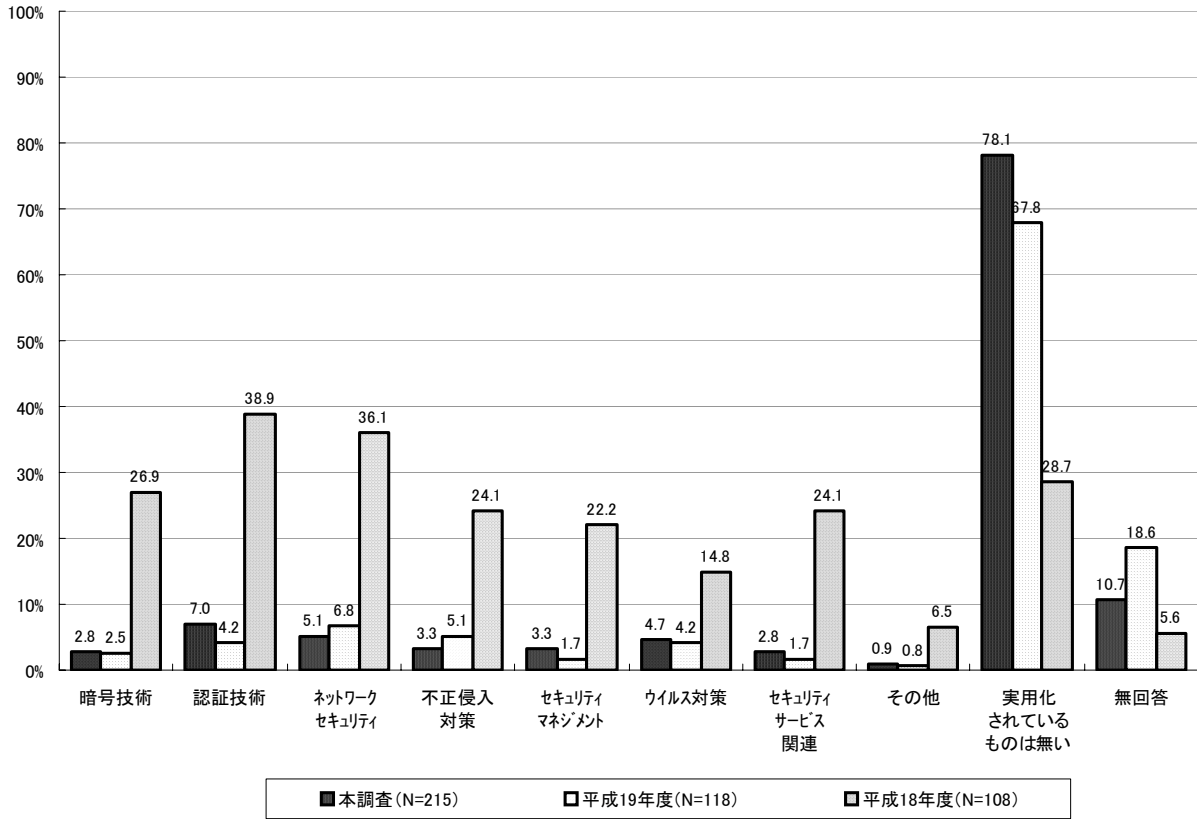
【本調査】現在、実用化(製品化)されているアクセス制御機能(MA)



【経年比較（全体）】

各分野とも 3～7%程度となっており、全体的な傾向は昨年度と大きな差は見られない。昨年度の上位分野であった「認証技術」と「ネットワークセキュリティ」は今年度においても上位 2 位を占めている。

【経年比較(全体)】現在、実用化(製品化)されているアクセス制御機能(MA)

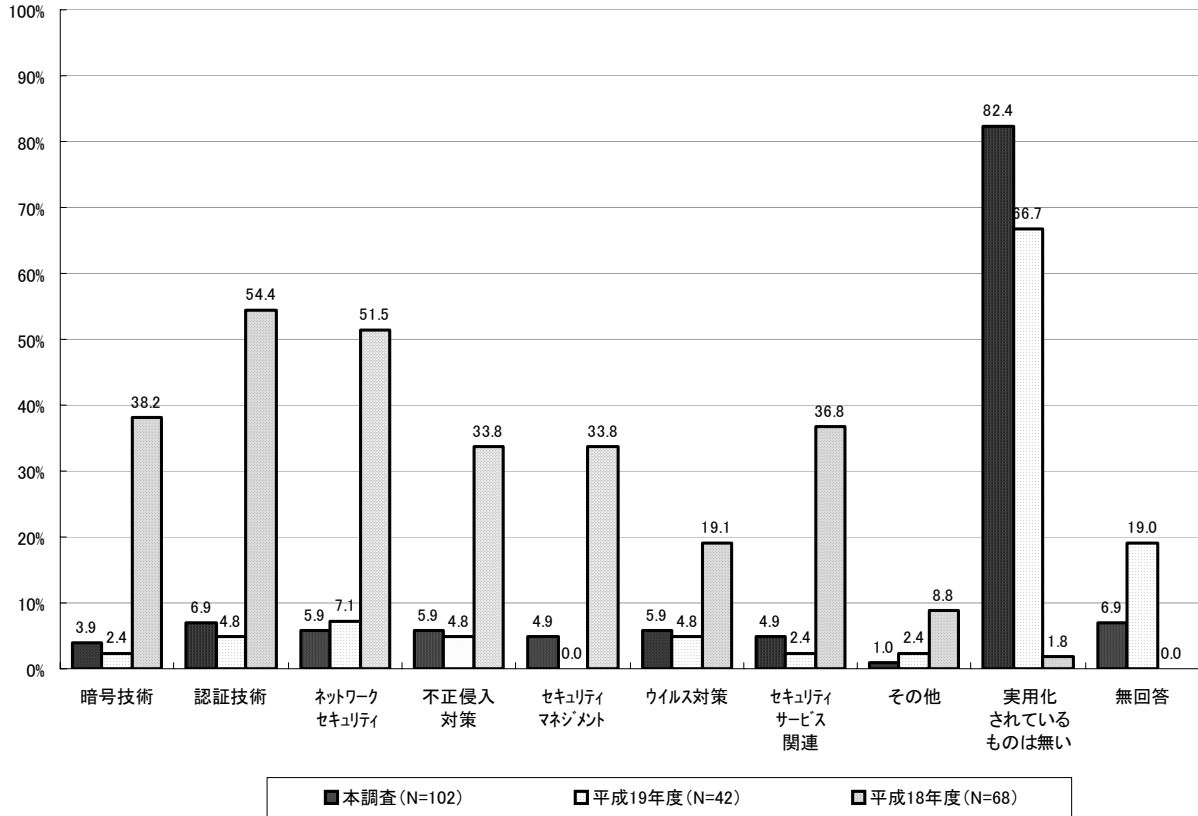




【経年比較（企業）】

各分野とも5%前後に分布しているが、その中でも「認証技術」が6.9%（7件）で最上位となっている。

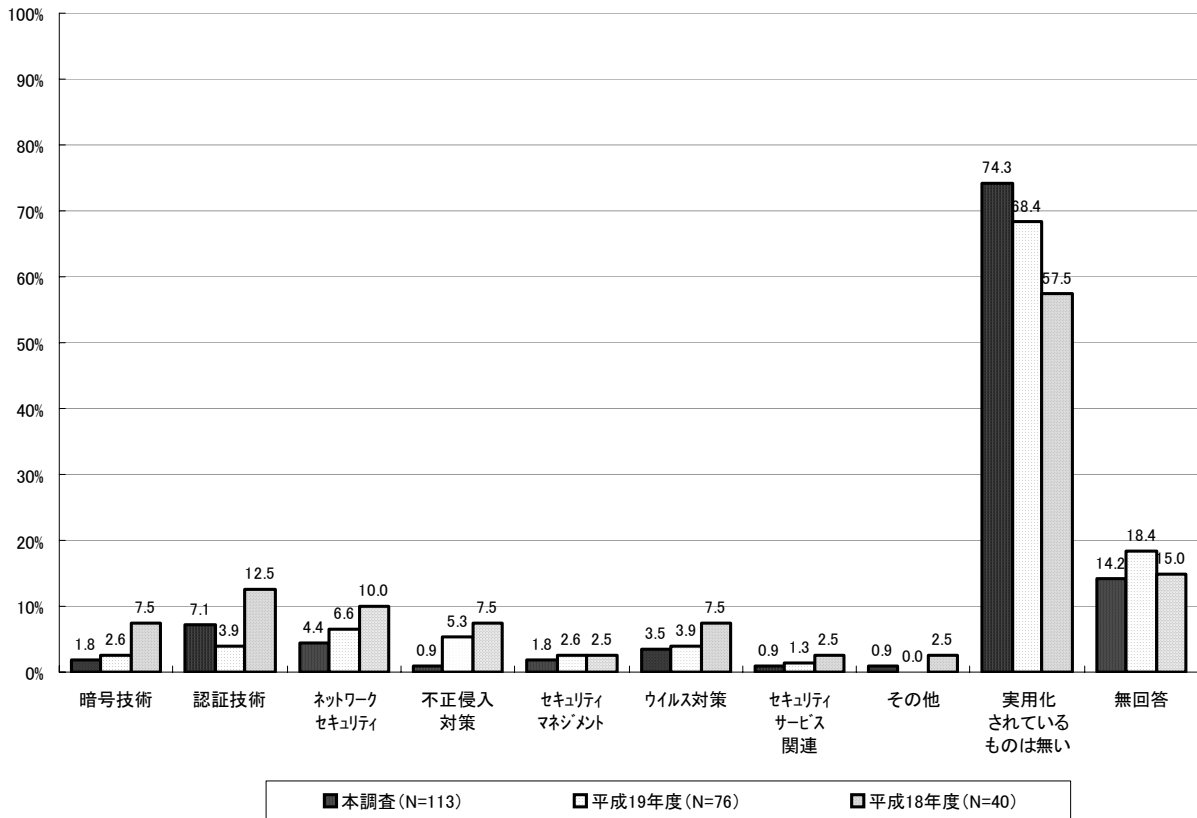
【経年比較(企業)】現在、実用化(製品化)されているアクセス制御機能(MA)



【経年比較（大学）】

大学において実用化されているものをみると、「認証技術」が7.1%（8件）と最も割合が高く、次いで「ネットワークセキュリティ」が4.4%（5件）、「ウイルス対策」が3.5%（4件）と続く。

【経年比較（大学）】現在、実用化（製品化）されているアクセス制御機能(MA)



## 1.6 今後、実用化（製品化）を見込んでいるアクセス制御機能

### 【本調査】

- 今後、実用化（製品化）を見込んでいるアクセス制御機能として、全体では回答の多い順に、「認証技術」「ネットワークセキュリティ」「セキュリティサービス関連」と続いている。

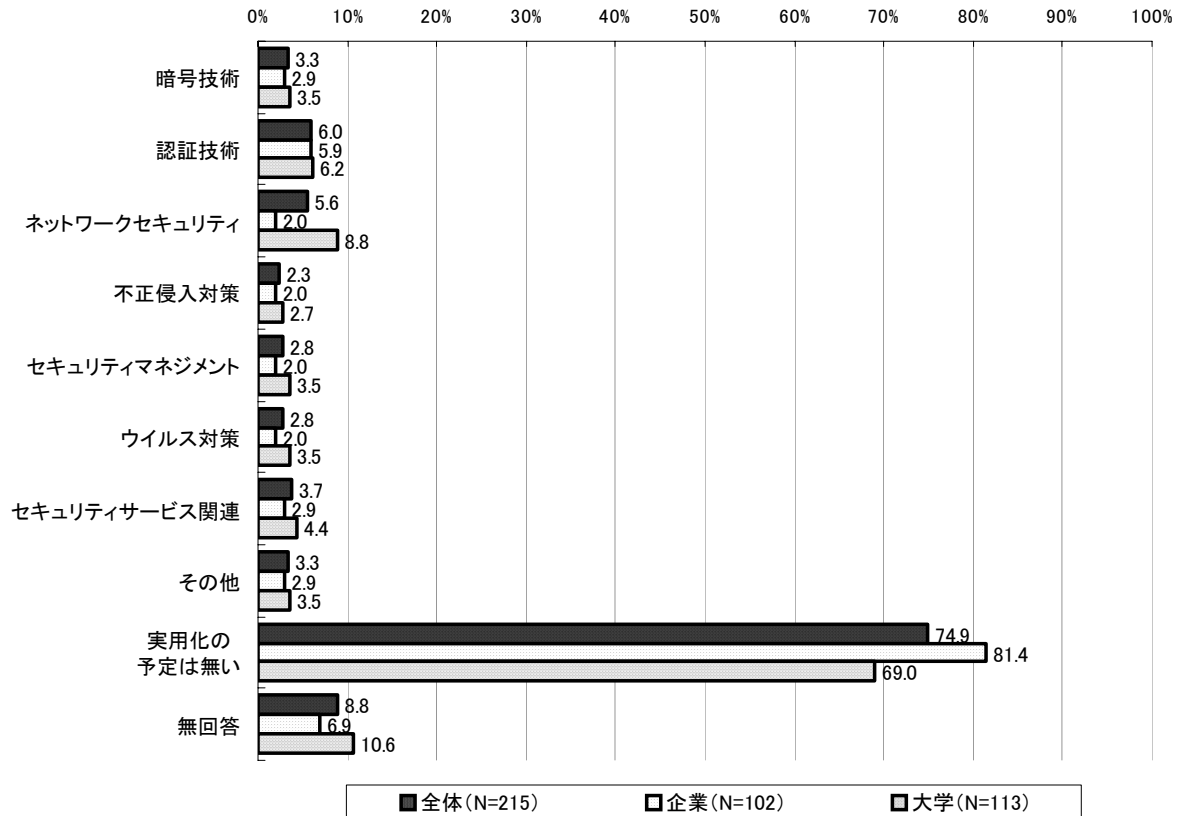
### 【経年比較】

- 「認証技術」を最多として、「ネットワークセキュリティ」「セキュリティサービス関連」が続いており、昨年度とほぼ同様の傾向である。

【本調査】

今後、実用化（製品化）を見込んでいるアクセス制御機能として、全体では「認証技術」が6.0%（13件）と最も高く、次いで「ネットワークセキュリティ」が5.6%（12件）、「セキュリティサービス関連」が3.7%（8件）と続く。

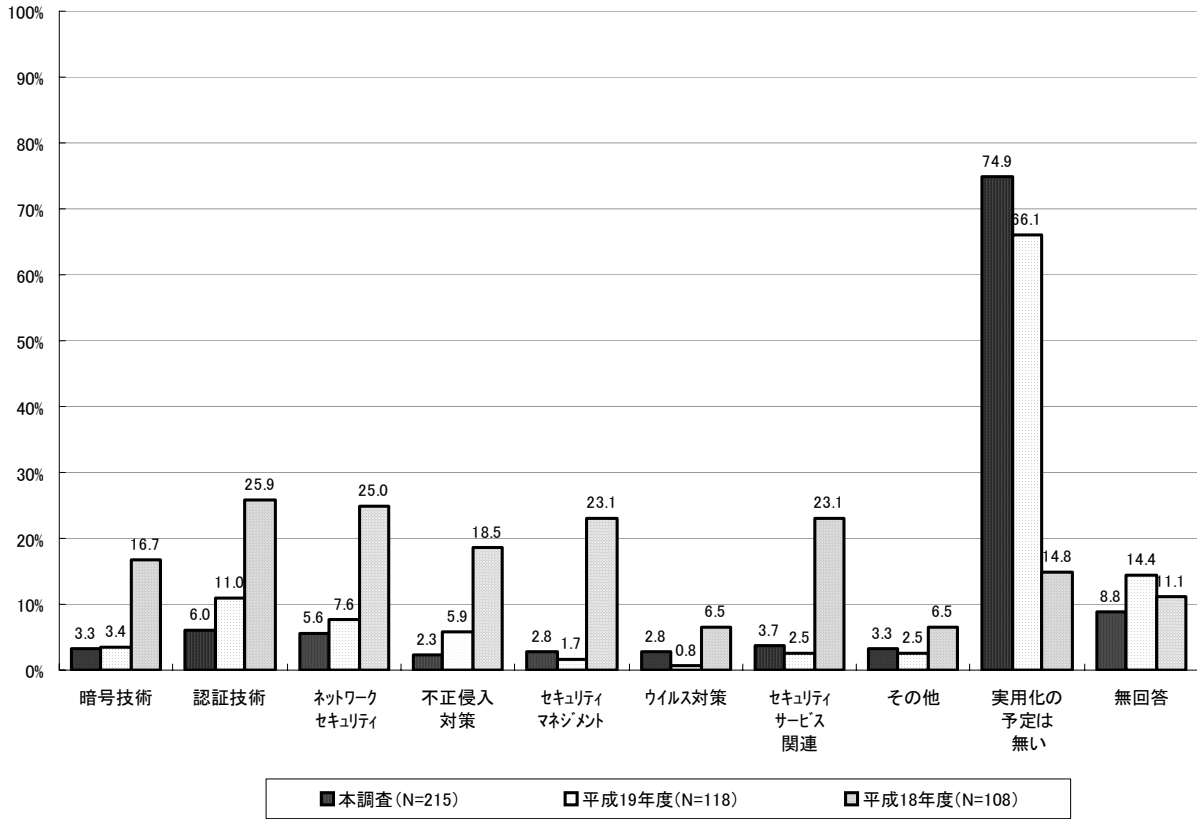
【本調査】今後、実用化（製品化）を見込んでいるアクセス制御機能(MA)



【経年比較（全体）】

「認証技術」の6.0%（13件）を最多として、「ネットワークセキュリティ」が5.6%（12件）、「セキュリティサービス関連」が3.7%（8件）と続いており、昨年度とほぼ同様の傾向と言える。

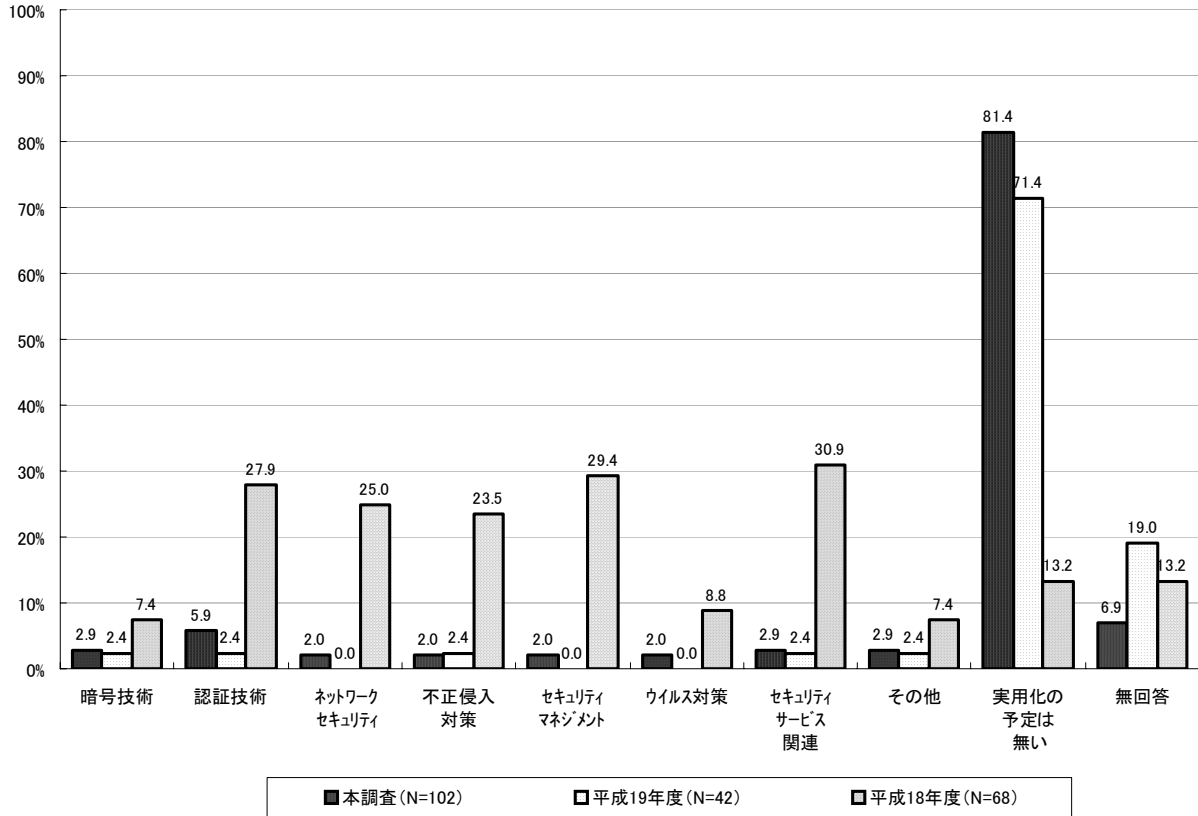
【経年比較（全体）】今後、実用化（製品化）を見込んでいるアクセス制御機能(MA)



【経年比較（企業）】

昨年度の有効回答数が少なく、経年での傾向把握は難しいものの、「認証技術」「暗号技術」「セキュリティサービス関連」に回答が集まっている点は昨年度と同様と言える。

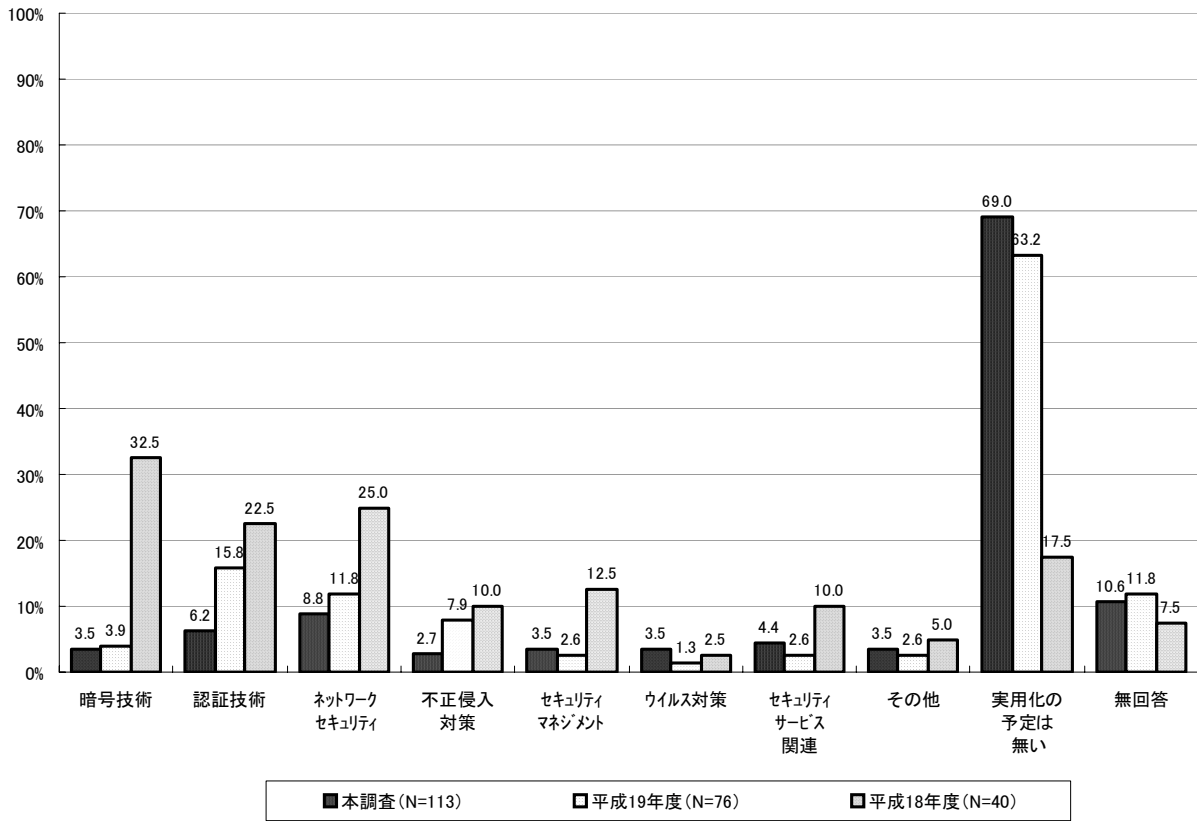
【経年比較（企業）】今後、実用化（製品化）を見込んでいるアクセス制御機能（MA）



【経年比較（大学）】

大学についてみると、昨年度と同様、「ネットワークセキュリティ」や「認証技術」においての実用化が見込まれている。「不正侵入対策」については今年度が2.7%（3件）と昨年度に比べ相対的に順位を下げている。

【経年比較(大学)】今後、実用化(製品化)を見込んでいるアクセス制御機能(MA)



## 2. 実用化された製品及び研究開発中の技術・サービス

本節では、回答用紙B（実用化（製品化））及び回答用紙C（研究開発）の各々の状況について、一覧表にまとめたものを示す。この一覧表は、バイヤーズガイドのような製品一覧表として使うことを想定しておらず、あくまで今回の調査対象とした大学・企業の母集団で抽出できたものを参考までに掲載したものである。この資料で一般的な傾向を知るなど、具体的な製品を選択する際の参考として使われたい。

また、表中の「技術開発状況」及び「概要・特徴など」については、回答をそのまま、または簡略化して掲載しており、調査者の意見を示すものではない。

### 2.1 ネットワークを守る

#### ①「技術の研究開発状況」

ネットワークに関する研究開発は、回答数が11件であり、認証技術に関する研究開発が主流となっている。ネットワークの異常検知に関する研究やコンテンツの流通制御、フィルタリングルールの最適化などの事例が挙げられている。

[2.1 ネットワークを守る]

企業・大学名	会津大学
代表者名	角山 茂章
所在地	〒965-8580 福島県会津若松市一箕町
窓口部署名 / 電話番号	
関連部門名	情報基礎論講座
URL	<a href="http://www.u-aizu.ac.jp/official/index_j.html">http://www.u-aizu.ac.jp/official/index_j.html</a>
対象技術	技術開発状況
研究開発名称： メッセージング・ネットワーク 情報基盤	content-based routing,mediationなどの技術をXML-routing装置等を用いて実装している。認証・許可・評価に基づいたコンテンツのアクセス制御、フォーマット変換などについて論文発表や実証実験を行っている。IDポータビリティへの応用も検討・開発・実験中。
研究開発国： 日本	
研究開発期間： H18.11.1～	



企業・大学名	秋田県立大学 システム科 学技術学部
代表者名	小林 淳
所在地	〒015-0055 秋田県由利本荘市土谷字海老ノ口84-4
窓口部署名 / 電話番号	電子情報システム学科 / 0184-27-2070
関連部門名	情報ネットワーク工学研究室
URL	http://www.akita-pu.ac.jp/
対象技術	技術開発状況
<b>研究開発名称 :</b> <b>ネットワークの異常検知に関する研究</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H17.4.1 ~ H22.3.31</b>	<p>アクセス制御機能の関連する研究開発として、(1)統計的性質を利用した一定時間内での攻撃パケットの有無の検知手法、(2)パケット解析に基づいた攻撃パケットの検知手法、および(3)アドレス偽装パケットの送信元特定に関する基礎的な研究を行っており、これまで一定の成果が得られている。</p> <p>(1)に関しては、ネットワーク出入り口で観測した実トラフィックデータに対し、通常時とは異なる状態が発生している場合、実測値を元にポアソン分布でモデル化したトラフィックデータと実測値との間にずれが大きくなることを利用し、DoS攻撃を含む異常検知手法として研究を行っている。(2)に関しては、ネットワーク側出入り口において、双方向の通信を観測することで送信元アドレスが偽装された不正な通信が行われたことを検知する手法である。(3)は、不正なアドレスパケットの送信やなりすましを行っているマシンの検知を行うための手法であり、管理しているネットワーク内部から送信元アドレスが偽装されたパケットが送信された場合、調査パケットをネットワーク内で送し応答パケットから不正マシンを特定する。(2)(3)は攻撃パケットを送信するウイルスに感染したマシンの検知にも応用可能である。</p>

企業・大学名	岡山大学 工学部
代表者名	野木 茂次
所在地	〒700-8530 岡山県岡山市津島中3-1-1
窓口部署名 / 電話番号	総務課 / 086-251-8002
関連部門名	通信ネットワーク工学科
URL	
対象技術	技術開発状況
<b>研究開発名称 :</b> <b>匿名認証技術</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.4.1 ~ H22.3.31</b>	<p>匿名認証技術の基盤となるグループ署名技術の開発を完了。本技術を組み込んだWebアクセス制御プロトコルや無線ネットワークアクセス制御プロトコルを実装中。</p>

企業・大学名	神奈川大学
代表者名	田中 賢
所在地	〒259-1293 神奈川県平塚市土屋2946
窓口部署名 / 電話番号	理学部 情報科学科 / 0463-59-4111(内線2838)
関連部門名	田中研究室
URL	http://www.kanagawa-u.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> フィルタリングルール最適化法  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H20.4.1 ~ H22.3.31	既に、パケットフィルタを構成する各ルールを論理式の集合としてモデル化し、フィルタリング負荷を軽減するルール再構成法を明らかにしている。 現在は、ルール間の関係が再構成アルゴリズムの計算量にどのような影響を与えるかを明らかにしている。これを基に、負荷軽減のための多項式時間アルゴリズムを考案している。

企業・大学名	岐阜大学 工学部
代表者名	工学部長 若井 和憲
所在地	〒501-1193 岐阜県岐阜市柳戸1-1
窓口部署名 / 電話番号	
関連部門名	岐阜大学 工学部 原山研究室
URL	
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> NZDSの解析に関する研究  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H20.4.1 ~ H23.3.31	IDSを利用したセキュリティ確保の手法のアイデアを貯めている段階

企業・大学名	東京農工大学
代表者名	学長 小畑 秀文
所在地	〒183-8538 東京都府中市晴見町3-8-1
窓口部署名 / 電話番号	学術情報チーム情報係 / 042-367-5526
関連部門名	
URL	http://www.tuat.ac.jp/
対象技術	技術開発状況
<b>研究開発名称 :</b> <b>P2Pネットワークにおけるコンテンツ流通制御</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H20.4.1 ~ H23.3.31</b>	<p>現在、インターネット機密情報が漏洩することがしばしば重大な問題となっている。その原因として、ファイル共有アプリケーションの利用が挙げられる。ファイル共有アプリケーションの多くは、ピアP2P(ピアツーピア)ネットワークを構成し、ファイルを共有するための情報を交換する。高いスケラビリティを提供するピアP2Pネットワークを用いたシステムは、将来有望な技術である。その一方で、P2Pネットワークには管理するシステムがなく、自律分散制御が行われるために、一度システムが動き出すと制御不能になる問題がある。たとえば、ピアP2Pを用いたファイル共有システムにおいては、一度ネットワークに流出したコンテンツファイルは回収不能になり、情報流出の問題を大きくする原因となっている。ファイル流出の問題を軽減するために、P2Pネットワーク上に偽のファイル、もしくは偽の情報を流して、流出してしまったファイルの流通を制御するポイズニング方式を開発している。日本で人気のあるピアP2Pファイル共有アプリケーションであるWinny,Shareおよび、海外でよく用いられるeDonkey,Limewire等を対象として有効なポイズニング方式を開発し、その効果を評価中である。特に分散ポイズニング方式、分散測定評価システムの開発によりスケラブルで、かつ効率のよいシステムの実現を目指している。</p>

企業・大学名	豊橋技術科学大学
代表者名	榊 佳之
所在地	〒411-8580 愛知県豊橋市天伯町雲雀ヶ丘1-1
窓口部署名 / 電話番号	総務課 総務係 / 0532-44-6504
関連部門名	工学部 情報工学系
URL	http://www.tut.ac.jp
対象技術	技術開発状況
<b>研究開発名称 :</b> <b>分散協調型攻撃検知・防御基盤</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H18.10 ~</b>	<ul style="list-style-type: none"> <li>・複数拠点でのDarknet、Honeynetの構築</li> <li>・収集Dataの解析</li> <li>・分散強調による防御・攻撃回避技術の基礎と開発中</li> </ul>

企業・大学名	宮崎大学 工学部
代表者名	中澤 隆雄
所在地	〒889-2192 宮崎県宮崎市学園木花台西1-1
窓口部署名 / 電話番号	工学部 庶務係 / 0985-58-2871
関連部門名	工学部 情報システム工学科
URL	http://www.miyazaki-u.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>IPトレースバックの効率化</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b>	<p>IPトレースバック技術の一つであるマーキング手法について、マーキング確率を動的に制御することにより、その効率を向上させる方法等について提案した。</p>

企業・大学名	武蔵工業大学
代表者名	中村 英夫
所在地	〒158-8557 東京都世田谷区玉堤1-28-1
窓口部署名 / 電話番号	情報処理センター / 03-3703-3111
関連部門名	情報処理センター研究室
URL	http://www.musashi-tech.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>AIPSを応用した検疫システム</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.4.1 ~ H21.3.31</b>	<p>すでに実用化している認証ネットワークシステムAIPSを応用し、クライアントのセキュリティパッチ適用状態やウイルス対策ソフトのパターン更新状況などを検査して、不適合な場合はネットワークから隔離する検疫システムである。現在、Windows XpとLinuxに対応しており、動作検証を行っている。</p>

企業・大学名	名城大学
代表者名	
所在地	〒468-8502 愛知県名古屋市長区塩釜口1-501
窓口部署名 / 電話番号	
関連部門名	理工学部 情報工学科
URL	http://www.meijo-u.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>フレキシブルプライベートネットワーク</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H14.10.1 ~ H22.3.31</b>	表題:フレキシブルプライベートネットワーク 内容:通信グループの定義を1度行えば、ユーザーがどのように移動しても管理負荷が発生しない。通信グループのメンバーは、認証後、暗号化通信を行う。状況:論文誌、掲載8件。研究会発表、約50件。ベンチャー企業(3社)の製品に一部機能の組み込みを検討中。

企業・大学名	三井情報株式会社
代表者名	
所在地	〒105-6215 東京都港区愛宕2-5-1 愛宕グリーンヒルズMORIタワー
窓口部署名 / 電話番号	事業開発本部 エンジニアリング部 / 03-6376-1040
関連部門名	事業開発本部 エンジニアリング部
URL	http://www.mki.co.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>IPv6認証サーバ</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H20.4.1 ~ H21.3.31</b>	IPv6インターネット接続環境にての認証基盤の利用拡大に向けての研究開発を行う。サービスの提供から記録までの流れを、認証(Authentication)、承認(Authorization)、アカウントिंग(Accounting)の3つの段階に分けて提供するAAA(Authentication, Authorization, Accounting)モデルアーキテクチャーをベースとしたRADIUS(Remote Authentication Dial In User Service)プロトコルを実装したRADIUSサーバ・ソフトウェアのIPv6化。また、RADIUSの後継となる次世代AAAモデルアーキテクチャーであるDiameterサーバ・ソフトウェアのIPv6化。

## ②「技術の実用化（製品化）状況」

ネットワークを守る実用化（製品化）されている技術は、回答数 7 件であり、様々な手段により個人やネットワークに対する認証機能を強化することで不正アクセスの侵入を防ぐ製品が主流となっている。

[2.1 ネットワークを守る]

企業・大学名	信州大学 大学院 工学系研究科 セキュリティ学講座
代表者名	不破 泰
所在地	〒380-8553 長野県長野市若里4-17-1
窓口部署名 / 電話番号	信州大学 工学部 / 026-269-5476
URL	<a href="http://security.cs.shinshu-u.ac.jp/">http://security.cs.shinshu-u.ac.jp/</a>
対象技術	概要・特徴など
<b>製品名 :</b> 個人認証によるバーチャルなネットワークを構成する動的経路制御技術  <b>開発元 :</b> 信州大学  <b>開発国 :</b> 日本  <b>発売時期 :</b>	現在、インターネット等におけるセキュアな通信の確保には、VPNを用いた暗号通信路が一般的である。しかし、VPNは装置を対向で利用することが前提であるため、データベースセンター側のVPN装置に障害が発生した場合、そのVPNを経由する全ての通信が途絶してしまう問題がある。更にVPNは接続する2点間に1つの暗号通信路を作り、全ての通信がこの通信路を共有する為、同じ暗号通信路を使う他の通信の傍受が容易である他、端末の操作者に応じてサービスを制限する事が出来ない等の問題がある。そこで、操作者の権利に応じて限定されたサービスを行う個別の暗号通信路を動的に確保するシステム(PCC:Private Certificated Connection)を新たに開発した。また、PCCにおける、個人認証をベースとして個別暗号通信路を開設するプロトコルの開発を行い、動的経路制御技術と併せてPCCを完成させた。また、プロトコルのシミュレーションと性能評価を実施した。要素技術として、動的な経路確保と認証局に関する技術開発で得られた要素技術を組み合わせ、個人認証をベースとしたアプリケーション単位での暗号化通信路の確保に関する技術開発を行った。さらに、RSA公開鍵暗号方式を用いた個人認証をベースに、アプリケーション対アプリケーションで利用される個別の暗号化通信路を、通信要求に応じて動的に開設・経路制御するプロトコルの実装を行った。この暗号化通信路の開設要求に対し、操作者の権利に応じてその開設を制御するために個人認証局の開発も行った。

企業・大学名	東京工業大学 学術国際情報センター
代表者名	渡邊 治
所在地	〒152-8550 東京都目黒区大岡山2-12-1
窓口部署名 / 電話番号	研究情報部情報基盤課 / 03-5734-3962
URL	http://www.gsic.titech.ac.jp
対象技術	概要・特徴など
<b>製品名 :</b> <b>キャンパス共通認証許可システム</b>  <b>開発元 :</b> <b>NTTコミュニケーションズ</b>  <b>開発国 :</b> <b>日本</b>  <b>発売時期 :</b>	<p>ICカード身分証を用いたPKIクライアント認証とウェブシングルサインオンシステムを組み合わせ、さまざまなウェブアプリケーションにセキュアかつ効率的に誘導するシステム。特徴としては、ICカードリーダーがない環境で補助的に利用するマトリクスコード認証機構を設けたこと、また、運用管理の負荷に関して考慮したことが挙げられる。</p>

企業・大学名	武蔵工業大学
代表者名	中村 英夫
所在地	〒158-8557 東京都世田谷区玉堤1-28-1
窓口部署名 / 電話番号	情報処理センター / 03-3703-3111
URL	http://www.musashi-tech.ac.jp
対象技術	概要・特徴など
<b>製品名 :</b> <b>Authenticated IP System</b>  <b>開発元 :</b> <b>武蔵工業大学</b>  <b>開発国 :</b> <b>日本</b>  <b>発売時期 :</b> <b>H20.10</b>	<p>AIPSは認証ネットワークシステムの一つで、IPヘッダに認証情報を埋め込むことでアクセス制御を実現している。クライアントにはWindows XPとLinuxが対応しており、ソフトウェアをインストールする必要がある。サーバはLinuxで、ゲートウェイとして機能する。特別な機器を必要とせず、一般的なハブなどの環境でも使用可能なため、低コストでの認証ネットワークを実現できる。</p>

企業・大学名	スカパーJSAT株式会社
代表者名	秋山 政徳
所在地	〒107-0052 東京都港区赤坂1-14-14
窓口部署名 / 電話番号	
URL	<a href="http://www.sptvjsat.com/">http://www.sptvjsat.com/</a>
対象技術	概要・特徴など
製品名 : インターネットVPNサービス	弊社向けに構築してもらったシステム及びネットワーク環境である為、以下詳細情報は記載出来ません。
開発元 : セコムトラストネット	
開発国 : 日本	
発売時期 :	

企業・大学名	トレンドマイクロ株式会社
代表者名	エバ・チェン
所在地	〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー
窓口部署名 / 電話番号	プロダクトマーケティング本部 / 03-5334-3600
URL	<a href="http://trendmicro.com/jp/home">http://trendmicro.com/jp/home</a>
対象技術	概要・特徴など
製品名 : 上記URL参照	上記URL参照
開発元 : トレンドマイクロ株式会社	
開発国 : 日本、アメリカ、中国他	
発売時期 :	



企業・大学名	株式会社ブロードバンドタワー
代表者名	大和 敏彦
所在地	〒107-0052 東京都港区赤坂4-2-6 住友不動産新赤坂ビル7F
窓口部署名 / 電話番号	人事総務部 / 03-5573-8181(代表)
URL	http://www.bbtower.co.jp
対象技術	概要・特徴など
製品名 : NetGuard(サービス)	1. 既存サイト全域へのサービス提供 2. 高いサービスへの継続性を確保 3. 接続条件に依存しないサービス 4. 短納期、およびスポット対応の実現 * 詳細は上記URL参照
開発元 :	
開発国 :	
発売時期 : H20.9	

企業・大学名	三井情報株式会社
代表者名	
所在地	〒105-6215 東京都港区愛宕2-5-1 愛宕グリーンヒルズMORIタワー
窓口部署名 / 電話番号	事業開発本部 エンジニアリング部 / 03-6376-1040
URL	http://www.mki.co.jp
対象技術	概要・特徴など
製品名 : NextCom RADIUSシリーズ	サービスの提供から記録までの流れを、認証(Authentication)、承認(Authorization)、アカウントリング(Accounting)の3つの段階に分けて提供するAAA(Authentication、Authentication、Authorization)モデルアーキテクチャーをベースとしたRADIUS(Remote Authentication Dial In User Service)プロトコルを実装したサーバ・ソフトウェア・シリーズです。また、ワンタイム・パスワード認証機能のサポートやローミング機能などを始めとする各種拡張機能を備え、Windows版では、ODBCサポートによるリレーショナルデータベースとの連携(アカウントリング出力)も可能です。ユーザ・アクティビティの容易な分析(アカウントログの多様な出力形式)や、正確な課金情報の収集等、現在の市場ニーズにも対応したRADIUSサーバ・管理ソフトウェアです。IEEE802.1xとEAPを用いたよりセキュアなネットワーク環境の構築を行うサーバ・ソフトウェア・パッケージも提供しています。
開発元 : 三井情報株式会社	
開発国 : 日本	
発売時期 : H10.4	

## 2.2 サーバを守る

### ①「技術の研究開発状況」

サーバに関する研究開発は、回答数 18 件で、DoS 攻撃に対する対策や、人間の記憶の仕組みや性質を生かしたものなど、様々な手段による認証技術の研究開発が進められている。

[2.2 サーバを守る]

企業・大学名	会津大学
代表者名	角山 茂章
所在地	〒965-8580 福島県会津若松市一箕町
窓口部署名 / 電話番号	
関連部門名	情報基礎論講座
URL	<a href="http://www.u-aizu.ac.jp/official/index_j.html">http://www.u-aizu.ac.jp/official/index_j.html</a>
対象技術	<b>技術開発状況</b>
研究開発名称： メッセージング・ネットワーク 情報基盤	content-based routing,mediationなどの技術をXML-routing装置等を用いて実装している。認証・許可・評価に基づいたコンテンツのアクセス制御、フォーマット変換などについて論文発表や実証実験を行っている。IDポータビリティへの応用も検討・開発・実験中。
研究開発国： 日本	
研究開発期間： H18.11.1 ~	

[2.2 サーバを守る]

企業・大学名	秋田県立大学 システム科 学技術学部
代表者名	小林 淳
所在地	〒015-0055 秋田県由利本荘市土谷字海老ノ口84-4
窓口部署名 / 電話番号	電子情報システム学科 / 0184-27-2070
関連部門名	情報ネットワーク工学研究室
URL	<a href="http://www.akita-pu.ac.jp/">http://www.akita-pu.ac.jp/</a>
対象技術	<b>技術開発状況</b>
研究開発名称： ネットワークの異常検知に関する研究	アクセス制御機能の関連する研究開発として、(1)統計的性質を利用した一定時間内での攻撃パケットの有無の検知手法、(2)パケット解析に基づいた攻撃パケットの検知手法、および(3)アドレス偽装パケットの送信元特定に関する基礎的な研究を行っており、これまで一定の成果が得られている。
研究開発国： 日本	(1)に関しては、ネットワーク出入り口で観測した実トラフィックデータに対し、通常時とは異なる状態が発生している場合、実測値を元にポアソン分布でモデル化したトラフィックデータと実測値との間にずれが大きくなることを利用し、DoS攻撃を含む異常検知手法として研究を行っている。(2)に関しては、ネットワーク側出入り口において、双方向の通信を観測することで送信元アドレスが偽装された不正な通信が行われたことを検知する手法である。(3)は、不正なアドレスパケットの送信やなりすましを行っているマシンの検知を行うための手法であり、管理しているネットワーク内部から送信元アドレスが偽装されたパケットが送信された場合、調査パケットをネットワーク内で送し応答パケットから不正マシンを特定する。(2)(3)は攻撃パケットを送信するウィルスに感染したマシンの検知にも応用可能である。
研究開発期間： H17.4.1 ~ H22.3.31	

企業・大学名	岡山大学 工学部
代表者名	野木 茂次
所在地	〒700-8530 岡山県岡山市津島中3-1-1
窓口部署名 / 電話番号	総務課 / 086-251-8002
関連部門名	通信ネットワーク工学科
URL	
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>匿名認証技術</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.4.1 ~ H22.3.31</b>	匿名認証技術の基盤となるグループ署名技術の開発を完了。本技術を組み込んだWebアクセス制御プロトコルや無線ネットワークアクセス制御プロトコルを実装中。

企業・大学名	神奈川工科大学 情報教育研究センター
代表者名	田辺 誠
所在地	〒243-0292 神奈川県厚木市下荻野1030
窓口部署名 / 電話番号	情報教育研究センター / 046-291-3224
関連部門名	情報教育研究センター 高速ネットワーク研究室
URL	
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>免疫系に学んだネットワーク異常検知システムの研究</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.4.1 ~</b>	生物の免疫系を参考にした免疫型ネットワーク異常検知理論の枠組みを構築し、研究室や大学内のネットワークトラフィックを用いて、シミュレーションにより提案した理論の有効性を評価している

企業・大学名	岐阜大学 工学部
代表者名	工学部長 若井 和憲
所在地	〒501-1193 岐阜県岐阜市柳戸1-1
窓口部署名 / 電話番号	
関連部門名	岐阜大学 工学部 原山研究室
URL	
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>NZDSの解析に関する研究</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H20.4.1 ~ H23.3.31</b>	IDSを利用したセキュリティ確保の手法のアイデアを貯めている段階

企業・大学名	近畿大学 工学部
代表者名	工学部長 京極 秀樹
所在地	〒739-2116 広島県東広島市高尾うめの辺1
窓口部署名 / 電話番号	工業技術研究所 / 082-434-7000(代表)
関連部門名	電子情報工学科 ネットワーク研究室
URL	<a href="http://www.hiro.kindai.ac.jp">http://www.hiro.kindai.ac.jp</a>
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>不正アクセスの検知とweb</b> <b>ファイルの自動修復</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H18.4.1 ~ H21.3.31</b>	システムを構築し、テスト段階

企業・大学名	芝浦工業大学
代表者名	柘植 綾夫
所在地	〒135-8548 東京都江東区豊洲3-7-5
窓口部署名 / 電話番号	総務部 / 03-5859-7000
関連部門名	情報ネットワーク
URL	http://www.shibaura-it.ac.jp
対象技術	<b>技術開発状況</b>
研究開発名称 : 公開制御	直接商用化、実用化は対象としていてよいが、実用化に供する基盤技術となるべく、シミュレーション等の評価実験により進めている。
研究開発国 : 日本	
研究開発期間 : H19.3.1 ~	

企業・大学名	東京工業大学 大学院 情報理工学研究科
代表者名	
所在地	〒152-8550 東京都目黒区大岡山2-12-1
窓口部署名 / 電話番号	
関連部門名	情報理工学研究科 千葉研
URL	http://www.ise.titech.ac.jp/
対象技術	<b>技術開発状況</b>
研究開発名称 : ファイルアクセス制御システム	URLを参照
研究開発国 : 日本	
研究開発期間 : H17.4.1 ~ H20.3.31	

企業・大学名	東邦大学 理学部 情報科学科
代表者名	
所在地	〒274-8510 千葉県船橋市三山2-2-1
窓口部署名 / 電話番号	047-472-8818
関連部門名	
URL	http://www.is.sci.toho-u.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>人間の記憶の特性を生かしたweb認証システム</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H18.4.10 ~ H21.3.20</b>	<p>現在、インターネットの普及・発達により、Webサイトがますます増加してきている。しかし、サイトの閲覧以外で何かサービスを受ける場合は、本人認証が必要となる場合が多い。その際に使用される本人認証は、文字パスワード認証を用いるのが一般的である。本研究では、パスワードによる認証を用いる方式で、「情動記憶」と「エピソード記憶」といった記憶の仕組みや性質をより活用することによって、ランダムで長い文字列でありながら長期に渡って覚えていられるパスワード認証システムを考案し、実験により評価した。被験者には、本研究認証システムを試してもらい、英数字8文字の文字パスワード認証システムとを比較して、1~28週間にわたって覚えていられるかを評価した。その結果、本研究認証システムの方が、長期覚えていられる認証システムであるという結果を得た。</p>

企業・大学名	徳島大学 工学部 知能情報工学科
代表者名	
所在地	〒770-8506 徳島県徳島市南常三島町2-1
窓口部署名 / 電話番号	
関連部門名	
URL	
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>情報資産マネージメントシステムの開発</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.4.1 ~ H21.3.31</b>	<p>情報資産情報を一元管理し、管理下の情報資産の中でサーバを監視、管理するWebアプリケーションの開発が終了した。</p>

企業・大学名	豊橋技術科学大学
代表者名	榊 佳之
所在地	〒411-8580 愛知県豊橋市天伯町雲雀ヶ丘1-1
窓口部署名 / 電話番号	総務課 総務係 / 0532-44-6504
関連部門名	工学部 情報工学系
URL	http://www.tut.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> 分散協調型攻撃検知・防御 <b>基盤</b>  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H18.10 ~	<ul style="list-style-type: none"> <li>・複数拠点でのDarknet、Honeynetの構築</li> <li>・収集Dataの解析</li> <li>・分散強調による防御・攻撃回避技術の基礎と開発中</li> </ul>

企業・大学名	法政大学
代表者名	増田 壽男
所在地	〒184-8584 東京都小金井市梶野町3-7-2
窓口部署名 / 電話番号	理工学部 応用情報工学科 / 042-387-6117
関連部門名	
URL	http://www.hosei.ac.jp/riko/joho/kyoin.html
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> 歩行認証技術  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H20.4.1 ~	歩行の様子をカメラで撮ることにより、本人かどうかを判別する技術である。今年着手したばかりである。

企業・大学名	前橋工科大学
代表者名	学長 江守 克彦
所在地	〒371-0816 群馬県前橋市上佐鳥町460-1
窓口部署名 / 電話番号	事務局 総務課 / 027-265-0111
関連部門名	情報システム研究室
URL	http://www.maebashi-it.ac.jp
対象技術	技術開発状況
<b>研究開発名称 :</b> <b>S-NIC</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.4.1 ~ H22.3.31</b>	<p>1.研究目的 DoS攻撃からサーバを保護するためには、正常なパケットと攻撃パケットを識別し、攻撃パケットを破棄する処理が必要である。攻撃パケットの識別は、攻撃パケットのシグネチャと、外部から到着するパケットをパターンマッチングにより比較することにより行われる。現在、このパターンマッチング処理はソフトウェアで行われることが多く、大規模なDoS攻撃を受けた際に処理能力が不足し、攻撃からサーバを保護できない。そこで近年、パターンマッチング処理をASIC化し、ハードウェアでパケットフィルタリングを行うことで処理能力を改善するアプローチ(以下、ハードウェアフィルタリングという)が行われるようになってきた。現在主流となっているのは、ハードウェアフィルタリング機能を搭載したIPS(Intrusion Prevention System)をネットワークにインラインで設置し、ネットワーク側からサーバを保護しようという方式である(図1)。これに対し、本研究では、NIC(Network Interface Card)にハードウェアフィルタリング機能を搭載し、制御用ソフトウェアと連携することでDoS攻撃に対処する手法を提案する(図2)。NICにハードウェアフィルタリング機能を付加することで得られる効果は次のとおりである。(1)ソフトウェアとの連携により、回路の小規模化や攻撃検出精度の向上が期待できる。(2)サーバごとにIPSが設置されているのと同等の構成となり、IPSの負荷分散効果が期待できる。(3)サーバごとにフィルタリングポリシーを決定できるため、きめ細かなフィルタリングが可能になる。</p> <div style="text-align: center;"> <p>図1 IPSによる防御</p> </div> <div style="text-align: center;"> <p>図2 提案する手法</p> </div> <p>2.研究計画 (1)実施計画 現在ハードウェアによるパターンマッチング処理には、連想メモリを使用する方法や、Aho-Corasick法によりパターンマッチングオートマトンを構築する方法などが用いられる。いずれの方法も、マッチングさせるルールが増加すると回路規模の増大を避けることができない。パケットフィルタリング処理をNICに搭載する際には、できるだけ回路規模の小さなパターンマッチング回路が必要となる。そこで本研究ではハードウェアとソフトウェアを連携させ、回路規模の増大を抑制すると共に、自由度の高いフィルタリングポリシーの適用が可能なパターンマッチング回路の開発を目指す。パターンマッチング回路は、ハードウェア記述言語VHDLにより記述し、回路シミュレータを使用して動作シミュレーションを行う。次にFPGAに実装し、処理速度や回路規模に関する評価を行う。(2)関連して行った研究 実験用に用意したWebサーバに対してDoS攻撃を行い、攻撃環境下におけるWebサーバの挙動を観察した。また、ソフトウェアによるDoS攻撃対策の有効性について評価を行った。DoS攻撃に対するパケットフィルタリングの有効性について検討するとともに、ハードウェアを用いたパケットフィルタリングについて、基本的なアーキテクチャを提案した。</p>



企業・大学名	宮崎大学 工学部
代表者名	中澤 隆雄
所在地	〒889-2192 宮崎県宮崎市学園木花台西1-1
窓口部署名 / 電話番号	工学部 庶務係 / 0985-58-2871
関連部門名	工学部 情報システム工学科
URL	http://www.miyazaki-u.ac.jp
対象技術	<b>技術開発状況</b>
研究開発名称 : IPTレースバックの効率化	IPTレースバック技術の一つであるマーキング手法について、マーキング確率を動的に制御することにより、その効率を向上させる方法等について提案した。
研究開発国 : 日本	
研究開発期間 :	

企業・大学名	武蔵工業大学
代表者名	中村 英夫
所在地	〒158-8557 東京都世田谷区玉堤1-28-1
窓口部署名 / 電話番号	情報処理センター / 03-3703-3111
関連部門名	情報処理センター研究室
URL	http://www.musashi-tech.ac.jp
対象技術	<b>技術開発状況</b>
研究開発名称 : AIPSを応用した検疫システム	すでに実用化している認証ネットワークシステムAIPSを応用し、クライアントのセキュリティパッチ適用状態やウイルス対策ソフトのパターン更新状況などを検査して、不適合な場合はネットワークから隔離する検疫システムである。現在、Windows XpとLinuxに対応しており、動作検証を行っている。
研究開発国 : 日本	
研究開発期間 : H19.4.1 ~ H21.3.31	

企業・大学名	明治大学 理工学部
代表者名	学部長 三木 一郎
所在地	〒214-8571 神奈川県川崎市多摩区東三田1-1-1
窓口部署名 / 電話番号	明治大学教務サービス部 理工学部グループ / 044-934-7559
関連部門名	理工学部 情報科学課
URL	http://www.meiji.ac.jp/sst/index.html
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> ユーザによる権限の分割・委譲 が可能なアクセス制御方式  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H18 ~ H20	プロトタイプの実装し、方式の検討中

企業・大学名	株式会社ブロードバンドタワー
代表者名	大和 敏彦
所在地	〒107-0052 東京都港区赤坂4-2-6 住友不動産新赤坂ビル7F
窓口部署名 / 電話番号	人事総務部 / 03-5573-8181(代表)
関連部門名	ネットワーク技術部
URL	http://www.bbtower.co.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b>   <b>研究開発国 :</b>   <b>研究開発期間 :</b> H20.11.1 ~ H22.10.31	・WAF製品の情報収集と機能確認 ・サービス要件、検討

企業・大学名	三井情報株式会社
代表者名	
所在地	〒105-6215 東京都港区愛宕2-5-1 愛宕グリーンヒルズMORIタワー
窓口部署名 / 電話番号	事業開発本部 エンジニアリング部 / 03-6376-1040
関連部門名	事業開発本部 エンジニアリング部
URL	http://www.mki.co.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>IPv6認証サーバ</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H20.4.1 ~ H21.3.31</b>	<p>IPv6インターネット接続環境にての認証基盤の利用拡大に向けての研究開発を行う。サービスの提供から記録までの流れを、認証(Authentication)、承認(Authorization)、アカウントिंग(Accounting)の3つの段階に分けて提供するAAA(Authentication、Authentication、Authorization)モデルアーキテクチャーをベースとしたRADIUS(Remote Authentication Dial In User Service)プロトコルを実装したRADIUSサーバ・ソフトウェアのIPv6化。また、RADIUSの後継となる次世代AAAモデルアーキテクチャーであるDiameterサーバ・ソフトウェアのIPv6化。</p>

## ②「技術の実用性（製品化）状況」

サーバを守る実用化（製品化）されている技術は、回答数 5 件であり、個別暗号通信路の開設、RSA 公開鍵暗号基盤などの、パスワード認証機能やネットワーク環境の強化のための開発が挙げられている。

[2.2 サーバを守る]

企業・大学名	信州大学 大学院 工学系研究科 セキュリティ学講座
代表者名	不破 泰
所在地	〒380-8553 長野県長野市若里4-17-1
窓口部署名 / 電話番号	信州大学 工学部 / 026-269-5476
URL	http://security.cs.shinshu-u.ac.jp/
対象技術	概要・特徴など
<b>製品名 :</b> 個人認証によるバーチャルなネットワークを構成する動的経路制御技術  <b>開発元 :</b> 信州大学  <b>開発国 :</b> 日本  <b>発売時期 :</b>	<p>現在、インターネット等におけるセキュアな通信の確保には、VPNを用いた暗号通信路が一般的である。しかし、VPNは装置を対向で利用することが前提であるため、データベースセンター側のVPN装置に障害が発生した場合、そのVPNを経由する全ての通信が途絶してしまう問題がある。更にVPNは接続する2点間に1つの暗号通信路を作り、全ての通信がこの通信路を共有する為、同じ暗号通信路を使う他の通信の傍受が容易である他、端末の操作者に応じてサービスを制限する事が出来ない等の問題がある。そこで、操作者の権利に応じて限定されたサービスを行う個別の暗号通信路を動的に確保するシステム(PCC:Private Certificated Connection)を新たに開発した。また、PCCにおける、個人認証をベースとして個別暗号通信路を開設するプロトコルの開発を行い、動的経路制御技術と併せてPCCを完成させた。また、プロトコルのシミュレーションと性能評価を実施した。要素技術として、動的な経路確保と認証局に関する技術開発で得られた要素技術を組み合わせ、個人認証をベースとしたアプリケーション単位での暗号化通信路の確保に関する技術開発を行った。さらに、RSA公開鍵暗号方式を用いた個人認証をベースに、アプリケーション対アプリケーションで利用される個別の暗号化通信路を、通信要求に応じて動的に開設・経路制御するプロトコルの実装を行った。この暗号化通信路の開設要求に対し、操作者の権利に応じてその開設を制御するために個人認証局の開発も行った。</p>

企業・大学名	東京工業大学 学術国際情報センター
代表者名	渡邊 治
所在地	〒152-8550 東京都目黒区大岡山2-12-1
窓口部署名 / 電話番号	研究情報部情報基盤課 / 03-5734-3962
URL	http://www.gsic.titech.ac.jp
対象技術	概要・特徴など
<b>製品名 :</b> キャンパス共通認証許可システム  <b>開発元 :</b> NTTコミュニケーションズ  <b>開発国 :</b> 日本  <b>発売時期 :</b>	ICカード身分証を用いたPKIクライアント認証とウェブシングルサインオンシステムを組み合わせ、さまざまなウェブアプリケーションにセキュアかつ効率的に誘導するシステム。特徴としては、ICカードリーダーがない環境で補助的に利用するマトリクスコード認証機構を設けたこと、また、運用管理の負荷に関して考慮したことが挙げられる。

企業・大学名	スカパーJSAT株式会社
代表者名	秋山 政徳
所在地	〒107-0052 東京都港区赤坂1-14-14
窓口部署名 / 電話番号	
URL	http://www.sptvjsat.com/
対象技術	概要・特徴など
<b>製品名 :</b> インターネットVPNサービス  <b>開発元 :</b> セコムトラストネット  <b>開発国 :</b> 日本  <b>発売時期 :</b>	弊社向けに構築してもらったシステム及びネットワーク環境である為、以下詳細情報は記載出来ません。

企業・大学名	トレンドマイクロ株式会社
代表者名	エバ・チェン
所在地	〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー
窓口部署名 / 電話番号	プロダクトマーケティング本部 / 03-5334-3600
URL	http://trendmicro.com/jp/home
対象技術	概要・特徴など
製品名 : 上記URL参照	上記URL参照
開発元 : トレンドマイクロ株式会社	
開発国 : 日本、アメリカ、中国他	
発売時期 :	

企業・大学名	三井情報株式会社
代表者名	
所在地	〒105-6215 東京都港区愛宕2-5-1 愛宕グリーンヒルズMORIタワー
窓口部署名 / 電話番号	事業開発本部 エンジニアリング部 / 03-6376-1040
URL	http://www.mki.co.jp
対象技術	概要・特徴など
製品名 : NextCom RADIUSシリーズ	サービスの提供から記録までの流れを、認証(Authentication)、承認(Authorization)、アカウントリング(Accounting)の3つの段階に分けて提供するAAA(Authentication、Authentication、Authorization)モデルアーキテクチャーをベースとしたRADIUS(Remote Authentication Dial In User Service)プロトコルを実装したサーバ・ソフトウェア・シリーズです。また、ワンタイム・パスワード認証機能のサポートやローミング機能などを始めとする各種拡張機能を備え、Windows版では、ODBCサポートによるリレーショナルデータベースとの連携(アカウントリング出力)も可能です。ユーザ・アクティビティの容易な分析(アカウントログの多様な出力形式)や、正確な課金情報の収集等、現在の市場ニーズにも対応したRADIUSサーバ・管理ソフトウェアです。IEEE802.1xとEAPを用いたよりセキュアなネットワーク環境の構築を行うサーバ・ソフトウェア・パッケージも提供しています。
開発元 : 三井情報株式会社	
開発国 : 日本	
発売時期 : H10.4	

## 2.3 クライアント（PC）を守る

### ①「技術の研究開発状況」

クライアント（PC）に関する研究開発は、回答数 14 件であり、個人認証や情報漏えい対策に関する研究が主流になっている。生物の免疫系を参考にしたネットワーク異常検知システムやネットワークトラフィック解析による不正アクセス検出法等が開発されている。

[2.3 クライアントを守る]

企業・大学名	会津大学
代表者名	角山 茂章
所在地	〒965-8580 福島県会津若松市一箕町
窓口部署名 / 電話番号	
関連部門名	情報基礎論講座
URL	<a href="http://www.u-aizu.ac.jp/official/index_j.html">http://www.u-aizu.ac.jp/official/index_j.html</a>
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>メッセージング・ネットワーク                  情報基盤</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H18.11.1 ~</b>	content-based routing,mediationなどの技術をXML-routing装置等を用いて実装している。認証・許可・評価に基づいたコンテンツのアクセス制御、フォーマット変換などについて論文発表や実証実験を行っている。IDポータビリティへの応用も検討・開発・実験中。

[2.3 クライアントを守る]

企業・大学名	岡山大学 工学部
代表者名	野木 茂次
所在地	〒700-8530 岡山県岡山市津島中3-1-1
窓口部署名 / 電話番号	総務課 / 086-251-8002
関連部門名	通信ネットワーク工学科
URL	
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>匿名認証技術</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.4.1 ~ H22.3.31</b>	匿名認証技術の基盤となるグループ署名技術の開発を完了。本技術を組み込んだWebアクセス制御プロトコルや無線ネットワークアクセス制御プロトコルを実装中。

企業・大学名	神奈川県立 情報教育研究センター
代表者名	田辺 誠
所在地	〒243-0292 神奈川県厚木市下荻野1030
窓口部署名 / 電話番号	情報教育研究センター / 046-291-3224
関連部門名	情報教育研究センター 高速ネットワーク研究室
URL	
対象技術	技術開発状況
<b>研究開発名称 :</b> 免疫系に学んだネットワーク異常検知システムの研究  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H19.4.1 ~	生物の免疫系を参考にした免疫型ネットワーク異常検知理論の枠組みを構築し、研究室や大学内のネットワークトラフィックを用いて、シミュレーションにより提案した理論の有効性を評価している

企業・大学名	高知大学 理学部
代表者名	川村 和夫
所在地	〒780-8520 高知県高知市曙町2-5-1
窓口部署名 / 電話番号	応用理学科情報コース
関連部門名	理学部 応用理学科 情報コース 森研究室
URL	<a href="http://www.is.kochi-u.ac.jp/">http://www.is.kochi-u.ac.jp/</a>
対象技術	技術開発状況
<b>研究開発名称 :</b> 追認証(バイオメトリクスを用いた)  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H15.4.1 ~	基礎実験中。



企業・大学名	芝浦工業大学
代表者名	柘植 綾夫
所在地	〒135-8548 東京都江東区豊洲3-7-5
窓口部署名 / 電話番号	総務部 / 03-5859-7000
関連部門名	情報ネットワーク
URL	http://www.shibaura-it.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>公開制御</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.3.1 ~</b>	直接商用化、実用化は対象としていてよいが、実用化に供する基盤技術となるべく、シミュレーション等の評価実験により進めている。

企業・大学名	徳島大学 工学部 知能情報工学科
代表者名	
所在地	〒770-8506 徳島県徳島市南常三島町2-1
窓口部署名 / 電話番号	
関連部門名	
URL	
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>情報資産マネージメントシステムの開発</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.4.1 ~ H21.3.31</b>	情報資産情報を一元管理し、管理下の情報資産の中でサーバを監視、管理するWebアプリケーションの開発が終了した。

企業・大学名	豊橋技術科学大学
代表者名	榊 佳之
所在地	〒411-8580 愛知県豊橋市天伯町雲雀ヶ丘1-1
窓口部署名 / 電話番号	総務課 総務係 / 0532-44-6504
関連部門名	工学部 情報工学系
URL	http://www.tut.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> 分散協調型攻撃検知・防御 <b>基盤</b>  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H18.10 ~	<ul style="list-style-type: none"> <li>・複数拠点でのDarknet、Honeynetの構築</li> <li>・収集Dataの解析</li> <li>・分散強調による防御・攻撃回避技術の基礎と開発中</li> </ul>

企業・大学名	法政大学
代表者名	増田 壽男
所在地	〒184-8584 東京都小金井市梶野町3-7-2
窓口部署名 / 電話番号	理工学部 応用情報工学科 / 042-387-6117
関連部門名	
URL	http://www.hosei.ac.jp/riko/joho/kyoin.html
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> 歩行認証技術  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H20.4.1 ~	歩行の様子をカメラで撮ることにより、本人かどうかを判別する技術である。今年着手したばかりである。

企業・大学名	前橋工科大学
代表者名	江守 克彦
所在地	〒371-0816 群馬県前橋市上佐鳥町460-1
窓口部署名 / 電話番号	事務局 総務課 / 027-265-0111
関連部門名	工学部 情報工学科
URL	http://www.maebashi-it.ac.jp
対象技術	<b>技術開発状況</b>
研究開発名称 : 迷惑メール対策ソフト	学生の教育を含む基礎研究です。
研究開発国 : 日本	
研究開発期間 :	

企業・大学名	三重大学大学院 工学研究科
代表者名	工学研究科長 武田 保雄
所在地	〒514-8507 三重県津市栗真町屋町1577
窓口部署名 / 電話番号	工学部・工学研究科チーム 総務担当 / 059-231-9466
関連部門名	三重大学 工学部 情報工学科 コンピューターネットワーク研究室
URL	http://www.eng.mie-u.ac.jp
対象技術	<b>技術開発状況</b>
研究開発名称 : ネットワークトラフィック解析と不正アクセス検出	ネットワークトラフィックを解析して不正アクセスを検出する手法を開発している。現在、収集したパケットの解析と、ニューラルネットワークなどの機械学習システムを用いて不正アクセス検出の実験を行っている。
研究開発国 : 日本	
研究開発期間 : H19.4.1 ~	

企業・大学名	武蔵工業大学
代表者名	中村 英夫
所在地	〒158-8557 東京都世田谷区玉堤1-28-1
窓口部署名 / 電話番号	情報処理センター / 03-3703-3111
関連部門名	情報処理センター研究室
URL	http://www.musashi-tech.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>AIPSを応用した検疫システム</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.4.1 ~ H21.3.31</b>	<p>すでに実用化している認証ネットワークシステムAIPSを応用し、クライアントのセキュリティパッチ適用状態やウイルス対策ソフトのバージョン更新状況などを検査して、不適合な場合はネットワークから隔離する検疫システムである。現在、Windows XpとLinuxに対応しており、動作検証を行っている。</p>

企業・大学名	明治大学 理工学部
代表者名	学部長 三木 一郎
所在地	〒214-8571 神奈川県川崎市多摩区東三田1-1-1
窓口部署名 / 電話番号	明治大学教務サービス部 理工学部グループ / 044-934-7559
関連部門名	理工学部 情報科学課
URL	http://www.meiji.ac.jp/sst/index.html
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>ユーザによる権限の分割・委譲 が可能なアクセス制御方式</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H18 ~ H20</b>	<p>プロトタイプの実装し、方式の検討中</p>

企業・大学名	株式会社 エイアンドティー
代表者名	磯村 健二
所在地	〒220-0005 神奈川県横浜市西区南幸2-20-5
窓口部署名 / 電話番号	LIS / 045-317-1507
関連部門名	LISユニット
URL	<a href="http://www.aandt.co.jp">http://www.aandt.co.jp</a>
対象技術	<b>技術開発状況</b>
研究開発名称 : 株式会社 エイアンドティー	シチズン時計の製品を検査システムに組み込みして認証デバイスとして試験段階になっています。シチズン時計株式会社の製品は以下のURLになります。(CertifGate)
研究開発国 : 日本	
研究開発期間 :	

企業・大学名	トレンドマイクロ株式会社
代表者名	エバ・チェン
所在地	〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー
窓口部署名 / 電話番号	プロダクトマーケティング本部 / 03-5334-3600
関連部門名	
URL	<a href="http://trendmicro.com/jp/home">http://trendmicro.com/jp/home</a>
対象技術	<b>技術開発状況</b>
研究開発名称 :	2009年より随時製品化予定。
研究開発国 :	
研究開発期間 :	

## ②「技術の実用化（製品化）状況」

クライアント（PC）を守る実用化（製品化）されている技術は、回答数 2 件であり、認証基盤のセキュリティ強化が主流と言える。パスワードなどの知識による認証のみならず、生体情報や所有物による認証システムなどの製品化も進められている。

[2.3 クライアントを守る]

企業・大学名	株式会社ディー・ディー・エス
代表者名	三吉野 健滋
所在地	〒450-0003 愛知県名古屋市中村区名駅南1-27-2 日本生命笹島ビル16F
窓口部署名 / 電話番号	開発本部 / 052-533-1110
URL	http://www.dds.co.jp/
対象技術	概要・特徴など
製品名 : EVE-MA	EVE-MAは、ActiveDirectoryを中心とした大規模ユーザ環境における認証基盤の役割を果たすソフトウェアである。 認証手段をプラグインとして追加できる構造を持ち、例えばパスワード等の知識に基づく認証、指紋に代表される生体情報による認証、FeliCa等のICカードを用いた所有物による認証を、アクセス先に応じた条件で組み合わせて認証できる特徴を持つ。 認証の実行はサーバ側に集約し、証明書ベースのサーバ・クライアント間の相互認証に基づいた認可を行う等、セキュリティを強く意識した構成としている。 なお、通信及び内部で用いる暗号については、電子政府推奨暗号リストに記載された暗号を全面的に採用している。
開発元 : 株式会社ディー・ディー・エス	
開発国 : 日本	
発売時期 : H19.11	

[2.3 クライアントを守る]

企業・大学名	トレンドマイクロ株式会社
代表者名	エバ・チェン
所在地	〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー
窓口部署名 / 電話番号	プロダクトマーケティング本部 / 03-5334-3600
URL	http://trendmicro.com/jp/home
対象技術	概要・特徴など
製品名 : 上記URL参照	上記URL参照
開発元 : トレンドマイクロ株式会社	
開発国 : 日本、アメリカ、中国他	
発売時期 :	

## 2.4 通信情報を守る

### ①「技術の研究開発状況」

通信情報に関する研究開発は、回答数7件であり、暗号システムについての開発が主流となっている。ネットワークの異常検知や機密保持通信を行うための暗号法や通信法の研究事例等が見受けられる。

[2.4 通信情報を守る]

企業・大学名	会津大学
代表者名	角山 茂章
所在地	〒965-8580 福島県会津若松市一箕町
窓口部署名 / 電話番号	
関連部門名	情報基礎論講座
URL	<a href="http://www.u-aizu.ac.jp/official/index_j.html">http://www.u-aizu.ac.jp/official/index_j.html</a>
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>メッセージング・ネットワーク情報基盤</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H18.11.1 ~</b>	content-based routing,mediationなどの技術をXML-routing装置等を用いて実装している。認証・許可・評価に基づいたコンテンツのアクセス制御、フォーマット変換などについて論文発表や実証実験を行っている。IDポータビリティへの応用も検討・開発・実験中。

[2.4 通信情報を守る]

企業・大学名	秋田県立大学 システム科 学技術学部
代表者名	小林 淳
所在地	〒015-0055 秋田県由利本荘市土谷字海老ノ口84-4
窓口部署名 / 電話番号	電子情報システム学科 / 0184-27-2070
関連部門名	情報ネットワーク工学研究室
URL	<a href="http://www.akita-pu.ac.jp/">http://www.akita-pu.ac.jp/</a>
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>ネットワークの異常検知に関する研究</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H17.4.1 ~ H22.3.31</b>	アクセス制御機能の関連する研究開発として、(1)統計的性質を利用した一定時間内での攻撃パケットの有無の検知手法、(2)パケット解析に基づいた攻撃パケットの検知手法、および(3)アドレス偽装パケットの送信元特定に関する基礎的な研究を行っており、これまで一定の成果が得られている。 (1)に関しては、ネットワーク出入り口で観測した実トラフィックデータに対し、通常時とは異なる状態が発生している場合、実測値を元にポアソン分布でモデル化したトラフィックデータと実測値との間にずれが大きくなることを利用し、DoS攻撃を含む異常検知手法として研究を行っている。(2)に関しては、ネットワーク側出入り口において、双方向の通信を観測することで送信元アドレスが偽装された不正な通信が行われたことを検知する手法である。(3)は、不正なアドレスパケットの送信やなりすましを行っているマシンの検知を行うための手法であり、管理しているネットワーク内部から送信元アドレスが偽装されたパケットが送信された場合、調査パケットをネットワーク内で送出し応答パケットから不正マシンを特定する。(2)(3)は攻撃パケットを送信するウィルスに感染したマシンの検知にも応用可能である。

企業・大学名	宇都宮大学 工学部
代表者名	進村 武男
所在地	〒321-8585 栃木県宇都宮市陽東7-1-2
窓口部署名 / 電話番号	総務係 / 028-689-6005
関連部門名	情報システム科学専攻
URL	
対象技術	<b>技術開発状況</b>
研究開発名称 : セキュアワイアレスアドホック ネットワーク	ワイヤレス アドホックネットワークは、インフラレスで無線が直接届かない端末間を他の端末を経由して通信するネットワークである。 ここで、中継端末における通信データの盗聴改ざんが問題となる。 本研究では、これを防止するためのトランスポート層以上のプロトコルの研究を進めている。
研究開発国 :	
研究開発期間 : H18.4 ~ H22.3	

企業・大学名	八戸工業大学
代表者名	学長 庄谷 征美
所在地	〒031-8501 青森県八戸市大字妙字大開88-1
窓口部署名 / 電話番号	事務部 庶務課 / 0178-25-8111
関連部門名	
URL	<a href="http://www.hi-tech.ac.jp/">http://www.hi-tech.ac.jp/</a>
対象技術	<b>技術開発状況</b>
研究開発名称 : カオス同期を用いた秘匿通信 システム	<ul style="list-style-type: none"> <li>・オープンなネットワーク利用が不可欠である現代の情報社会では、機密保持通信を行うための暗号法や通信法が研究されています。</li> <li>・カオスの応用研究も盛んで、送信側と受信側の二つのサブシステムを信号の送信時にのみカオス同期させ、その状態を暗号鍵とする方法があります。</li> <li>・カオス同期を用いたアナログかつハードウェアの秘匿通信システムが、製品化されました。</li> <li>・インターネット時代に適応したデジタルかつソフトウェアの秘匿通信システムを構築しています。</li> <li>・カオス同期を用いた通信手法では、サブシステムモデルが盗まれるとパラメータを特定される恐れがあります。</li> <li>・秘匿性向上に有効なシステムの設計法として、実際のカオス時系列から得られるファジィモデルを同期化部のモデルに用いる秘匿通信システムの構築法とそのシステムを用いた秘匿通信手法を研究中です。</li> <li>・カオス同期化部にファジィモデルを用い、カオス分岐パラメータを用いたカオス変調が、従来の秘匿カオス通信手法と同様に、実用可能か研究します。</li> <li>・同相変換量子化手法によって得られるカオス乱数と呼ばれるデジタル信号を用いることで、デジタル情報信号の秘匿カオス通信が、実用可能か研究します。</li> </ul>
研究開発国 :	
研究開発期間 : H20.4.1 ~ H22.3.31	



企業・大学名	明治大学 理工学部
代表者名	学部長 三木 一郎
所在地	〒214-8571 神奈川県川崎市多摩区東三田1-1-1
窓口部署名 / 電話番号	明治大学教務サービス部 理工学部グループ / 044-934-7559
関連部門名	理工学部 情報科学課
URL	<a href="http://www.meiji.ac.jp/sst/index.html">http://www.meiji.ac.jp/sst/index.html</a>
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> ユーザによる権限の分割・委譲 が可能なアクセス制御方式  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H18 ~ H20	プロトタイプの実装し、方式の検討中

企業・大学名	明星大学
代表者名	小川 哲生
所在地	〒191-8506 東京都日野市程久保2-1-1
窓口部署名 / 電話番号	企画課 / 042-591-5111
関連部門名	
URL	<a href="http://www.meisei-u.ac.jp">http://www.meisei-u.ac.jp</a>
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> ストリーム暗号の設計に関する研究  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H10 ~ H17	<ul style="list-style-type: none"> <li>・ストリーム暗号における非線形擬似乱数発生器の評価</li> <li>・カオス現象を応用した擬似乱数発生器の評価</li> <li>・内部メモリを持つ擬似乱数発生器の出力系列特性の評価</li> <li>・VHDLによるストリーム暗号の製作</li> </ul>

企業・大学名	株式会社ディー・ディー・エス
代表者名	三吉野 健滋
所在地	〒450-0003 愛知県名古屋市中村区名駅南1-27-2 日本生命笹島ビル16F
窓口部署名 / 電話番号	開発本部 / 052-533-1110
関連部門名	開発本部
URL	http://www.dds.co.jp/
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>追跡不能性を有した匿名認証システム</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H17.12 ~ H21.1.16</b>	<p>平成17年度・18年度経済産業省委託研究として、東京大学と共に開発してきた技術であり、ユビキタス環境での認証とプライバシー保護を両立する技術である。</p> <p>ユビキタス環境においては、シームレスなサービスの提供のために、アクセス制御のための認証が継続的に行われる必要がある。一方、従来の認証技術においては、認証の際には何らかのIDを提示する必要があり、このIDを基にして様々な場面での認証イベントを紐付けることによってユーザの追跡が可能となり、ユーザのプライバシーが脅かされる懸念があった。</p> <p>本技術では、ユーザを追跡できるようなIDを提示せずに認証を実施できる認証スキームを実現しており、年齢認証を代表とした属性認証などの用途への適応を進めている。</p>

## ②「技術の実用化（製品化）状況」

通信情報を守る実用化（製品化）されている技術は、回答数 3 件であり、暗号化や VPN などの技術が主流となっている。個人認証をベースとしたアプリケーション単位での暗号化通信路の確保に関する技術開発などが行われている。

[2.4 通信情報を守る]

企業・大学名	信州大学 大学院 工学系研究科 セキュリティ学講座
代表者名	不破 泰
所在地	〒380-8553 長野県長野市若里4-17-1
窓口部署名 / 電話番号	信州大学 工学部 / 026-269-5476
URL	http://security.cs.shinshu-u.ac.jp/
対象技術	概要・特徴など
<b>製品名 :</b> 個人認証によるバーチャルなネットワークを構成する動的経路制御技術  <b>開発元 :</b> 信州大学  <b>開発国 :</b> 日本  <b>発売時期 :</b>	<p>現在、インターネット等におけるセキュアな通信の確保には、VPNを用いた暗号通信路が一般的である。しかし、VPNは装置を対向で利用することが前提であるため、データベースセンター側のVPN装置に障害が発生した場合、そのVPNを経由する全ての通信が途絶してしまう問題がある。更にVPNは接続する2点間に1つの暗号通信路を作り、全ての通信がこの通信路を共有する為、同じ暗号通信路を使う他の通信の傍受が容易である他、端末の操作者に応じてサービスを制限する事が出来ない等の問題がある。そこで、操作者の権利に応じて限定されたサービスを行う個別の暗号通信路を動的に確保するシステム(PCC:Private Certificated Connection)を新たに開発した。また、PCCにおける、個人認証をベースとして個別暗号通信路を開設するプロトコルの開発を行い、動的経路制御技術と併せてPCCを完成させた。また、プロトコルのシミュレーションと性能評価を実施した。要素技術として、動的な経路確保と認証局に関する技術開発で得られた要素技術を組み合わせ、個人認証をベースとしたアプリケーション単位での暗号化通信路の確保に関する技術開発を行った。さらに、RSA公開鍵暗号方式を用いた個人認証をベースに、アプリケーション対アプリケーションで利用される個別の暗号化通信路を、通信要求に応じて動的に開設・経路制御するプロトコルの実装を行った。この暗号化通信路の開設要求に対し、操作者の権利に応じてその開設を制御するために個人認証局の開発も行った。</p>

企業・大学名	東京工業大学 学術国際情報センター
代表者名	渡邊 治
所在地	〒152-8550 東京都目黒区大岡山2-12-1
窓口部署名 / 電話番号	研究情報部情報基盤課 / 03-5734-3962
URL	<a href="http://www.gsic.titech.ac.jp">http://www.gsic.titech.ac.jp</a>
対象技術	概要・特徴など
製品名 : キャンパス共通認証許可システム	ICカード身分証を用いたPKIクライアント認証とウェブシングルサインオンシステムを組み合わせ、さまざまなウェブアプリケーションにセキュアかつ効率的に誘導するシステム。特徴としては、ICカードリーダーがない環境で補助的に利用するマトリクスコード認証機構を設けたこと、また、運用管理の負荷に関して考慮したことが挙げられる。
開発元 : NTTコミュニケーションズ	
開発国 : 日本	
発売時期 :	

企業・大学名	スカパーJSAT株式会社
代表者名	秋山 政徳
所在地	〒107-0052 東京都港区赤坂1-14-14
窓口部署名 / 電話番号	
URL	<a href="http://www.sptvjsat.com/">http://www.sptvjsat.com/</a>
対象技術	概要・特徴など
製品名 : インターネットVPNサービス	弊社向けに構築してもらったシステム及びネットワーク環境である為、以下詳細情報は記載出来ません。
開発元 : セコムトラストネット	
開発国 : 日本	
発売時期 :	

## 2.5 データを守る

### ①「技術の研究開発状況」

データに関する研究開発は、回答数 10 件であり、秘密分散技術や電子すかし、コンテンツの流通制御、追跡不能性を有した匿名認証のシステムなど、研究開発の状況は多岐にわたっていると言える。

[2.5 データを守る]

企業・大学名	会津大学
代表者名	角山 茂章
所在地	〒965-8580 福島県会津若松市一箕町
窓口部署名 / 電話番号	
関連部門名	情報基礎論講座
URL	<a href="http://www.u-aizu.ac.jp/official/index_j.html">http://www.u-aizu.ac.jp/official/index_j.html</a>
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>メッセージング・ネットワーク          情報基盤</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H18.11.1 ~</b>	content-based routing,mediationなどの技術をXML-routing装置等を用いて実装している。認証・許可・評価に基づいたコンテンツのアクセス制御、フォーマット変換などについて論文発表や実証実験を行っている。IDポータビリティへの応用も検討・開発・実験中。

[2.5 データを守る]

企業・大学名	愛媛大学大学院 理工学研究科
代表者名	甲斐 博
所在地	〒790-8577 愛媛県松山市文京町3
窓口部署名 / 電話番号	089-927-9956
関連部門名	愛媛大学 大学院 理工学研究科 甲斐 博
URL	<a href="http://www.hpc.cs.ehime-u.ac.jp/">http://www.hpc.cs.ehime-u.ac.jp/</a>
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>有理関数補間を用いた秘密          分散法の研究</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.4.1 ~</b>	分散情報の中に不正者が存在することを指摘するために、Rifaは有理関数補間を用いた秘密分散法を提案している。しかし、どれが不正かを特定できなかった。有利関数補間を用いた秘密分散法の再考察を行い、正しくない分散情報の特定を行う方法の研究を行っている。

企業・大学名	神奈川大学
代表者名	木下 宏揚
所在地	〒221-8686 神奈川県横浜市神奈川区六角橋3-27-1
窓口部署名 / 電話番号	木下研究室 / 045-481-5661
関連部門名	木下研究室
URL	http://www.kanagawa-u.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>情報セキュリティに関する研究</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H17.4.1 ~ H21.3.31</b>	理論的なモデルを検討中

企業・大学名	芝浦工業大学
代表者名	柘植 綾夫
所在地	〒135-8548 東京都江東区豊洲3-7-5
窓口部署名 / 電話番号	総務部 / 03-5859-7000
関連部門名	情報ネットワーク
URL	http://www.shibaura-it.ac.jp
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> <b>公開制御</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H19.3.1 ~</b>	直接商用化、実用化は対象としていてよいが、実用化に供する基盤技術となるべく、シミュレーション等の評価実験により進めている。

企業・大学名	東京農工大学
代表者名	学長 小畑 秀文
所在地	〒183-8538 東京都府中市晴見町3-8-1
窓口部署名 / 電話番号	学術情報チーム情報係 / 042-367-5526
関連部門名	
URL	http://www.tuat.ac.jp/
対象技術	技術開発状況
<b>研究開発名称 :</b> <b>P2Pネットワークにおけるコンテンツ流通制御</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H20.4.1 ~ H23.3.31</b>	<p>現在、インターネット機密情報が漏洩することがしばしば重大な問題となっている。その原因として、ファイル共有アプリケーションの利用が挙げられる。ファイル共有アプリケーションの多くは、ピアP2P(ピアツーピア)ネットワークを構成し、ファイルを共有するための情報を交換する。高いスケラビリティを提供するピアP2Pネットワークを用いたシステムは、将来有望な技術である。その一方で、P2Pネットワークには管理するシステムがなく、自律分散制御が行われるために、一度システムが動き出すと制御不能になる問題がある。たとえば、ピアP2Pを用いたファイル共有システムにおいては、一度ネットワークに流出したコンテンツファイルは回収不能になり、情報流出の問題を大きくする原因となっている。ファイル流出の問題を軽減するために、P2Pネットワーク上に偽のファイル、もしくは偽の情報を流して、流出してしまったファイルの流通を制御するポイズニング方式を開発している。日本で人気のあるピアP2Pファイル共有アプリケーションであるWinny,Shareおよび、海外でよく用いられるeDonkey,Limewire等を対象として有効なポイズニング方式を開発し、その効果を評価中である。特に分散ポイズニング方式、分散測定評価システムの開発によりスケラブルで、かつ効率のよいシステムの実現を目指している。</p>

企業・大学名	豊橋技術科学大学
代表者名	榊 佳之
所在地	〒411-8580 愛知県豊橋市天伯町雲雀ヶ丘1-1
窓口部署名 / 電話番号	総務課 総務係 / 0532-44-6504
関連部門名	工学部 情報工学系
URL	http://www.tut.ac.jp
対象技術	技術開発状況
<b>研究開発名称 :</b> <b>分散協調型攻撃検知・防御基盤</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H18.10 ~</b>	<ul style="list-style-type: none"> <li>・複数拠点でのDarknet、Honeynetの構築</li> <li>・収集Dataの解析</li> <li>・分散強調による防御・攻撃回避技術の基礎と開発中</li> </ul>

企業・大学名	明治大学 理工学部
代表者名	学部長 三木 一郎
所在地	〒214-8571 神奈川県川崎市多摩区東三田1-1-1
窓口部署名 / 電話番号	明治大学教務サービス部 理工学部グループ / 044-934-7559
関連部門名	理工学部 情報科学課
URL	<a href="http://www.meiji.ac.jp/sst/index.html">http://www.meiji.ac.jp/sst/index.html</a>
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> ユーザによる権限の分割・委譲 が可能なアクセス制御方式  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H18 ~ H20	プロトタイプの実装し、方式の検討中

企業・大学名	山口大学 大学院 理工学研究科(理学系)
代表者名	理学部長 増山 博行
所在地	〒753-8512 山口県山口市吉田1677-1
窓口部署名 / 電話番号	理学部 総務・予算係 / 083-933-5205
関連部門名	山口大学 理工学研究科
URL	<a href="http://www.sci.yamaguchi-u.ac.jp/">http://www.sci.yamaguchi-u.ac.jp/</a>
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> なし  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H20.4.1 ~	電子透かしに関する手法の開発および評価を行っている。



企業・大学名	立命館大学
代表者名	総長 川口 清史
所在地	〒604-8520 京都府京都市中京区西ノ京朱雀町1
窓口部署名 / 電話番号	総務部 広報課 / 075-813-8300
関連部門名	情報理工学部
URL	http://www.ritsumeijp/
対象技術	技術開発状況
<b>研究開発名称 :</b> <b>Privacy-aware OS Salvia</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H15.4.1 ~</b>	Linuxオペレーティングシステムを拡張し、ポリシーに基づいたファイルアクセス制御を実現するPrivacy-aware OS Salviaを研究・開発している。一般的に、安全性と利便性はトレードオフの関係にあるが、Salviaでは、企業などにおける通常業務を従来どおり可能としつつも、業務担当者によるデータの無断持ち出し(故意・ミス両方を含む)による情報漏洩を防止することを目的としているものである。Salviaは、それを実現するために、ポリシーはファイル毎に設定可能としている。ポリシーには大まかに、「同一ファイルへの出力」「元のファイル以外への出力」「リムーバブルメディアへの出力」「同一計算機内の他プログラムへの送信」「他の計算機のプログラムへの送信」について、そのファイルの内容を出力してよいかどうかを記述できる。プログラムがポリシー付きのファイルを読み書きすると、それ以降、プログラムはポリシーに記述された制約を受ける仕組みとなっている。例えば、同一ファイルへの出力のみが可と設定されたファイルがあるとすると、そのファイルをアクセスしたプログラムは別のファイルへの出力アクセスが禁止される。すなわち、当該データの参照や更新といった処理は可能となるが、それを別のファイルへコピーすることは不可能となる。現在、本システムの基本部分はほぼ完成しており、利用者環境で導入を容易にするための仕組みの構築を行っている。具体的には、本システムをLinuxSecurityModuleを用いた再構築や、ユーザプロセスとして実現するUser-modeSalviaの開発を行っている。

企業・大学名	株式会社ディー・ディー・エス
代表者名	三吉野 健滋
所在地	〒450-0003 愛知県名古屋市中村区名駅南1-27-2 日本生命笹島ビル16F
窓口部署名 / 電話番号	開発本部 / 052-533-1110
関連部門名	開発本部
URL	http://www.dds.co.jp/
対象技術	技術開発状況
<b>研究開発名称 :</b> <b>追跡不能性を有した匿名認証システム</b>  <b>研究開発国 :</b> <b>日本</b>  <b>研究開発期間 :</b> <b>H17.12 ~ H21.1.16</b>	平成17年度・18年度経済産業省委託研究として、東京大学と共に開発してきた技術であり、ユビキタス環境での認証とプライバシー保護を両立する技術である。ユビキタス環境においては、シームレスなサービスの提供のために、アクセス制御のための認証が継続的に行われる必要がある。一方、従来の認証技術においては、認証の際には何らかのIDを提示する必要があり、このIDを基にして様々な場面での認証イベントを紐付けることによってユーザの追跡が可能となり、ユーザのプライバシーが脅かされる懸念があった。本技術では、ユーザを追跡できるようなIDを提示せずに認証を実施できる認証スキームを実現しており、年齢認証を代表とした属性認証などの用途への適応を進めている。

## ②「技術の実用化（製品化）状況」

データを守る実用化（製品化）されている技術は、回答数 4 件となっている。学内外からの多数の利用者が混在する大学では、部外者からの組織内限定サービスへのアクセス保護を可能としたシステムの導入が進められている。

[2.5 データを守る]

企業・大学名	岡山大学
代表者名	千葉 喬三
所在地	〒700-8530 岡山県岡山市津島中1-1-1
窓口部署名 / 電話番号	総合情報基盤センター / 086-251-7231
URL	<a href="http://www.okayama-u.ac.jp/user/cc">http://www.okayama-u.ac.jp/user/cc</a>
対象技術	概要・特徴など
<p><b>製品名 :</b> 部外者からの組織内限定サービスへのアクセスを保護する LANアクセス制御システム</p> <p><b>開発元 :</b> 岡山大学総合情報基盤センター</p> <p><b>開発国 :</b> 日本</p> <p><b>発売時期 :</b> H17.8</p>	<p>大学などの組織においてLANアクセス環境を提供する場合、特に学会などのイベント開催時には組織内利用者とそれ以外の利用者(部外者)が混在して利用することが多い。このような場合、部外者でも組織内限定サービスを利用できるなどの問題が生じる。この問題に対して、本システムでは、部外者からの組織内限定サービスへのアクセス保護を、管理コストを増加させずに可能にする。すなわち、部外者が組織内限定サービスへアクセスした場合でも、サーバ側での設定に基づいたアクセス制御を行うことが可能である。また、本システムは既存の組織内ネットワークを利用するため、LANアクセス環境の提供が場所によらず容易に行えるという特徴を持つ。</p>

企業・大学名	東京工業大学 学術国際情報センター
代表者名	渡邊 治
所在地	〒152-8550 東京都目黒区大岡山2-12-1
窓口部署名 / 電話番号	研究情報部情報基盤課 / 03-5734-3962
URL	<a href="http://www.gsic.titech.ac.jp">http://www.gsic.titech.ac.jp</a>
対象技術	概要・特徴など
製品名 : キャンパス共通認証許可システム  開発元 : NTTコミュニケーションズ  開発国 : 日本  発売時期 :	ICカード身分証を用いたPKIクライアント認証とウェブシングルサインオンシステムを組み合わせ、さまざまなウェブアプリケーションにセキュアかつ効率的に誘導するシステム。特徴としては、ICカードリーダーがない環境で補助的に利用するマトリクスコード認証機構を設けたこと、また、運用管理の負荷に関して考慮したことが挙げられる。

企業・大学名	スカパーJSAT株式会社
代表者名	秋山 政徳
所在地	〒107-0052 東京都港区赤坂1-14-14
窓口部署名 / 電話番号	
URL	<a href="http://www.sptvjsat.com/">http://www.sptvjsat.com/</a>
対象技術	概要・特徴など
製品名 : インターネットVPNサービス  開発元 : セコムトラストネット  開発国 : 日本  発売時期 :	弊社向けに構築してもらったシステム及びネットワーク環境である為、以下詳細情報は記載出来ません。

企業・大学名	トレンドマイクロ株式会社
代表者名	エバ・チェン
所在地	〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー
窓口部署名 / 電話番号	プロダクトマーケティング本部 / 03-5334-3600
URL	<a href="http://trendmicro.com/jp/home">http://trendmicro.com/jp/home</a>
対象技術	概要・特徴など
製品名 : 上記URL参照	上記URL参照
開発元 : トレンドマイクロ株式会社	
開発国 : 日本、アメリカ、中国他	
発売時期 :	

## 2.6 施設を守る

### ①「技術の研究開発状況」

施設に関する研究開発は、回答数 2 件であり、人間の顔や歩行の様子を視覚的に捉えることによる認証技術の開発が進められている。

[2.6 施設を守る]

企業・大学名	日本女子大学 理学部
代表者名	
所在地	〒112-8681 東京都文京区目白台2-8-1
窓口部署名 / 電話番号	
関連部門名	日本女子大学 理学部
URL	http://www.jwu.ac.jp
対象技術	<b>技術開発状況</b>
研究開発名称 : 光認証システムによる顔、画像、動画認証	本研究開発は、光相関演算を利用し、超高速に顔認証を行うシステムを開発するものである。顔認証では、コンピュータログインから入退出管理、入出国審査などさまざまな応用用途がある。顔認証にとどまらず、一般的な動画・画像にも適用できるため、不正画像・動画監視にも利用できる。「動画検索のための超高速光サーバの小型化に関する研究開発」として、独立行政法人新エネルギー・産業技術総合開発機構(NEDO)大学発事業創出実用化研究開発、および「次世代光相関技術を用いた超高速画像情報検索・著作権管理技術の研究開発」総務省戦略的情報通信研究開発推進制度(SCOPE)による助成を受けて行っている。備考:これらの研究成果の一部は、警視庁・警察庁と連携し、以下のような発表会を行っており、いずれの発表会においても100名以上の参加を頂いた。更にこの顔認証システムは官房長官賞を受賞している。1.小館香椎子、渡邊恵理子、”光並列相関器によるバイオメトリクス顔認証—FARCOのデモストレーション—”、警視庁&警察庁研究発表会(2003.12)官房長官賞 2.小館香椎子、渡邊恵理子、”顔認証技術の現状と犯罪防止への応用”第31回 最先端技術講演会、警察庁(2006.3)
研究開発国 : 日本	
研究開発期間 :	

[2.6 施設を守る]

企業・大学名	法政大学
代表者名	増田 壽男
所在地	〒184-8584 東京都小金井市梶野町3-7-2
窓口部署名 / 電話番号	理工学部 応用情報工学科 / 042-387-6117
関連部門名	
URL	http://www.hosei.ac.jp/riko/joho/kyoin.html
対象技術	<b>技術開発状況</b>
研究開発名称 : 歩行認証技術	歩行の様子をカメラで撮ることにより、本人かどうかを判別する技術である。今年着手したばかりである。
研究開発国 : 日本	
研究開発期間 : H20.4.1 ~	

## ②「技術の実用化（製品化）状況」

施設を守る実用化（製品化）されている技術は、回答数 1 件であった。パスワードなどの知識による認証のみならず、生体情報や所有物による認証基盤のセキュリティ強化のためのシステムなどの製品化が進められている。

[2.6 施設を守る]

企業・大学名	株式会社ディー・ディー・エス
代表者名	三吉野 健滋
所在地	〒450-0003 愛知県名古屋市中村区名駅南1-27-2 日本生命笹島ビル16F
窓口部署名 / 電話番号	開発本部 / 052-533-1110
URL	http://www.dds.co.jp/
対象技術	概要・特徴など
<b>製品名 :</b> <b>EVE-MA</b>  <b>開発元 :</b> <b>株式会社ディー・ディー・エス</b>  <b>開発国 :</b> <b>日本</b>  <b>発売時期 :</b> <b>H19.11</b>	<p>EVE-MAは、ActiveDirectoryを中心とした大規模ユーザ環境における認証基盤の役割を果たすソフトウェアである。</p> <p>認証手段をプラグインとして追加できる構造を持ち、例えばパスワード等の知識に基づく認証、指紋に代表される生体情報による認証、FeliCa等のICカードを用いた所有物による認証を、アクセス先に応じた条件で組み合わせて認証できる特徴を持つ。</p> <p>認証の実行はサーバ側に集約し、証明書ベースのサーバ・クライアント間の相互認証に基づいた認可を行う等、セキュリティを強く意識した構成としている。</p> <p>なお、通信及び内部で用いる暗号については、電子政府推奨暗号リストに記載された暗号を全面的に採用している。</p>

## 2.7 その他

### ①「技術の研究開発状況」

その他に関する研究開発は、回答数 2 件となっている。先に述べたもの以外の研究開発としては、迷惑メールによるアドレス収集の防止対策、追跡不能性を有した匿名認証スキームなどの開発が進められている。

[2.7 その他]

企業・大学名	岡山大学
代表者名	千葉 喬三
所在地	〒700-8530 岡山県岡山市津島中1-1-1
窓口部署名 / 電話番号	総合情報基盤センター / 086-251-7231
関連部門名	情報基盤部門
URL	http://www.okayama-u.ac.jp/user/cc
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> 電子メールシステムにおけるアドレス収集防止機能の研究開発  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H17.4 ~	最近、電子メールシステムにおいて迷惑メールの蔓延が大きな社会問題になっている。迷惑メールの多くはハーベスティングと呼ばれる手法によって収集したアドレスに送られるため、迷惑メール送信者によるアドレス収集を防止することは迷惑メールの被害を軽減するために重要である。これに対して、我々の研究グループではすでに開発した電子メールの配送中に通信を強制切断する手法を応用し、アドレス収集を目的としていると推定される通信については宛先の存在確認を行わないようにする手法について、現在研究開発を進めている。

[2.7 その他]

企業・大学名	株式会社ディー・ディー・エス
代表者名	三吉野 健滋
所在地	〒450-0003 愛知県名古屋市中村区名駅南1-27-2 日本生命笹島ビル16F
窓口部署名 / 電話番号	開発本部 / 052-533-1110
関連部門名	開発本部
URL	http://www.dds.co.jp/
対象技術	<b>技術開発状況</b>
<b>研究開発名称 :</b> 追跡不能性を有した匿名認証システム  <b>研究開発国 :</b> 日本  <b>研究開発期間 :</b> H17.12 ~ H21.1.16	平成17年度・18年度経済産業省委託研究として、東京大学と共に開発してきた技術であり、ユビキタス環境での認証とプライバシー保護を両立する技術である。ユビキタス環境においては、シームレスなサービスの提供のために、アクセス制御のための認証が継続的に行われる必要がある。一方、従来の認証技術においては、認証の際には何らかのIDを提示する必要があり、このIDを基にして様々な場面での認証イベントを紐付けることによってユーザの追跡が可能となり、ユーザのプライバシーが脅かされる懸念があった。本技術では、ユーザを追跡できるようなIDを提示せずに認証を実施できる認証スキームを実現しており、年齢認証を代表とした属性認証などの用途への適応を進めている。

## ②「技術の実用化（製品化）状況」

当質問に関する回答は得られなかった。