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１７年１月

警察庁生活安全局情報技術犯罪対策課

目次

第１章

調査の概要

第1章　調査の概要

1. 調査の目的

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の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

調査対象は、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 件抽出した。

・大学（187 校）
　国立・私立大学から理工系学部を設置する大学から無作為に抽出
・上場企業等（127 社）
　上場企業のうち、業種分類が「情報・通信」「サービス」「電気機器」「金融」である企業から、セキュリティ製品・サービスを提供している企業から無作為に抽出
・NPO 日本ネットワークセキュリティ協会（JNSA）会員企業（187 社）

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：2004 年 10 月 6 日～12 月 22 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、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：巻末付属資料にある『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、ICカード、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、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

(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(ハードウエア、ソフトウエア、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：巻末付属資料の『回答用紙 B』『回答用紙 C』を参照

4. 送付、回収状況

送付数、回収数及び回収率は次のとおり。

	送付数	回収数	回収率(%)
企業	314	50	15.9%
大学	187	44	23.5%
合計	**501**	**94**	**18.8%**

回答用紙ごとの回収状況は次のとおり。

	回答用紙 A	回答用紙 B	回答用紙 C
企業	50	107	14
大学	44	2	16
回答数合計	**94**	**109**	**30**

第２章

調査結果
（概要と考察）

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（研究開発人員と研究開発費）

アクセス制御機能の技術研究開発に係る体制について、企業では「小規模化」若しくは「大規模化」の二極構造に、大学では、小規模でのユニット化の傾向が見られる。

研究開発人員に関する調査では、全体、企業および大学のいずれにおいても、アクセス制御機能の技術研究開発に人員を「投入できるところ」（１００人以上）と「投入できないところ」（０人若しくは１～４人）に偏在化しつつある。この傾向は平成１５年度調査との比較からも分かり、とくに大学では少人数化（１０人以下）に向かっている。

一方、研究開発費に関する調査では、全体、企業および大学のいずれにおいても、アクセス制御機能の技術研究開発に費用を「投下できるところ」（１億～１０億円）と「投下できないところ」（１，０００万円未満）に分化しつつある。平成１５年度調査との比較では、企業では上記の傾向が見られるが、大学では小額化に向かっている。

以上から、企業および大学におけるアクセス制御機能の技術研究開発に係る体制が「小規模化」若しくは「大規模化」の二極構造になりつつあり、とくに大学では小規模でのユニット化の傾向が見られる。

現在取り組んでいる分野を縦軸にとり、横軸に研究開発に携わっている人数に対する回答比率をとってみると、次の表のような結果となった。無回答を除き、比率の高い部分（上位 2 位あるいは 10%以上程度）を網掛けしてみたところ、数人(１～４人及び５～９人)の部分にピークが見られる。これは多くの組織での研究が、割と少人数で行われていることと符合する。

一方、100 人以上にもピークがいくつか現れており、暗号技術、認証技術、ウイルス対策で顕著である。この理由はもう少し精査する必要があるが、ウイルス対策は、アンチウイルスメーカなどが組織的に情報収集をしているなどの状況が反映されている可能性がある。

現在、取り組んでいる分　野	研究開発に携わっている人数							
	０人	１～４人	５～９人	１０～１９人	２０～４９人	５０～９９人	１００人～	無回答
暗号技術	3.57	14.29	10.71	7.14	3.57	0.00	14.29	46.43
認証技術	2.44	12.20	12.20	4.88	4.88	2.44	12.20	48.78
ネットワークセキュリティ	0.00	18.18	9.09	4.55	9.09	4.55	9.09	45.45
不正侵入対策	0.00	15.63	12.50	3.13	6.25	0.00	9.38	53.13
セキュリティマネジメント	2.94	20.59	8.82	8.82	5.88	2.94	5.88	44.12
ウイルス対策	0.00	11.54	7.69	0.00	7.69	0.00	15.38	57.69
セキュリティサービス関連	3.03	15.15	12.12	9.09	9.09	0.00	6.06	45.45
その他	0.00	16.67	0.00	0.00	16.67	8.33	0.00	58.33

(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

アクセス制御機能の技術研究開発に係る取り組み分野について、企業では「選択と集中」による「二極化」が見られる。また、「セキュリティマネジメント」、「認証技術」および「セキュリティサービス関連」に、今後、技術研究開発の重点が置かれると予想される。

現在、最も取り組まれている分野は、「ネットワークセキュリティ」（ネットワーク上の情報を保護・管理する技術）及び「認証技術」（コンピュータを利用しようとする本人を確認する技術）である。企業と大学では取り組み分野に差異が見られ、企業では「取り組み割合が比較的高い分野」と「取り組み割合が比較的低い分野」に分けることができ、取り組み分野に対する「選択と集中」が図られ、「二極化」が見られている。大学では、ほぼ全ての分野が平均的に取り組まれている。

また、今後、最も力を入れていく分野として、「セキュリティマネジメント」（情報セキュリティのための運用・管理手法）、「認証技術」および「セキュリティサービス関連」（情報セキュリティに関する評価・診断・監視）を挙げる企業・大学が多い。

さらに、本調査、平成１５年度調査および平成１４年度調査から、取り組み分野に係る今後の展望について推察する。「平成１４年度調査：今後、最も力を入れていく分野」→「平成１５年度調査：現在、取り組んでいる分野」、並びに「平成１５年度調査：今後、最も力を入れていく分野」→「本調査：現在、取り組んでいる分野」の比較から、「今後、最も力を入れていく分野」が直後の調査における「現在、取り組んでいる分野」に反映される可能性が高いと言える。この傾向から、本調査で「今後、最も力を入れていく分野」として上位に挙げられた「セキュリティマネジメント」、「認証技術」および「セキュリティサービス関連」に今後の重点がおかれると推察される。

【１】平成１４年度調査→平成１５年度調査→本調査のトレンドから、今後の研究開発の展望は？

【平成１４年度調査】全体
今後、最も力を入れていく分野

1	認証技術（24.6%）
2	ネットワークセキュリティ（23.0%）
3	セキュリティマネジメント（14.8%）
4	暗号技術（11.5%）
4	セキュリティサービス関連（11.5%）
6	不正侵入対策（6.6%）
7	ウイルス対策（1.6%）

【平成１５年度調査】全体
現在、取り組んでいる分野

1	認証技術（49.5%）
2	ネットワークセキュリティ（47.3%）
3	暗号技術（38.5%）
4	セキュリティマネジメント（34.1%）
5	セキュリティサービス関連（33.0%）
6	不正侵入対策（27.5%）
7	ウイルス対策（16.5%）

【平成１５年度調査】全体
今後、最も力を入れていく分野

1	ネットワークセキュリティ（23.1%）
2	認証技術（14.3%）
3	セキュリティマネジメント（12.1%）
4	セキュリティサービス関連（8.8%）
5	ウイルス対策（4.4%）
6	不正侵入対策（3.3%）
6	暗号技術（3.3%）

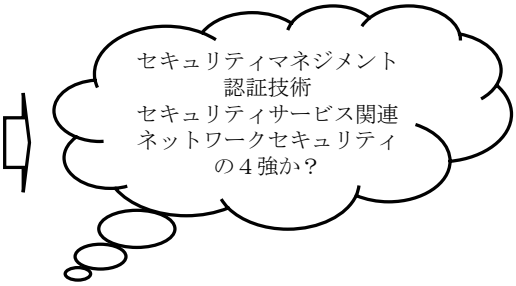
【本調査】全体
現在、取り組んでいる分野

1	ネットワークセキュリティ（43.6%）
2	認証技術（40.6%）
3	セキュリティマネジメント（33.7%）
4	セキュリティサービス関連（32.7%）
5	不正侵入対策（31.7%）
6	暗号技術（27.7%）
7	ウイルス対策（25.7%）

【本調査】全体
今後、最も力を入れていく分野

1	セキュリティマネジメント（11.9%）
2	認証技術（9.9%）
3	セキュリティサービス関連（8.9%）
4	ネットワークセキュリティ（7.9%）
5	暗号技術（5.0%）
6	不正侵入対策（1.0%）
7	ウイルス対策（0.0%）

【研究開発の今後の展望】
これまでの推移から



(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、「認証技術」、「セキュリティマネジメント」、「ネットワークセキュリティ」および「セキュリティサービス関連」が、今後、主流になると思われる。

現在、実用化（製品化）されているアクセス制御機能は、「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」および「セキュリティマネジメント」が多い。企業と大学では差異が見られ、企業では「実用化（製品化）の割合が比較的高い分野」と「実用化（製品化）の割合が比較的低い分野」に分けることができる。大学では、ほぼ全ての分野が同程度に実用化（製品化）がされているが、企業に比べると極めて低い。

また、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、「認証技術」、「セキュリティマネジメント」、「ネットワークセキュリティ」および「セキュリティサービス関連」を挙げる企業・大学が多い。

さらに、本調査、平成１５年度調査および平成１４年度調査から、実用化（製品化）に係る今後の展望について推察する。「平成１４年度調査：今後、実用化（製品化）を見込んでいる分野」→「平成１５年度調査：現在、実用化（製品化）されている分野」を見ると順位の入れ替わりが若干見られるが、「平成１５年度調査：今後、実用化（製品化）を見込んでいる分野」→「本調査：現在、実用化（製品化）されている分野」の比較から、「今後、実用化（製品化）を見込んでいる分野」が直後の調査における「現在、実用化（製品化）されている分野」におおむね反映されていると言える。この傾向から、本調査で「今後、実用化（製品化）を見込んでいる分野」として上位に挙げられた「認証技術」、「セキュリティマネジメント」、「ネットワークセキュリティ」および「セキュリティサービス関連」が今後の実用化（製品化）の主流になると推察される。

【２】平成１４年度調査→平成１５年度調査→本調査のトレンドから、今後の実用化（製品化）の展望は？

【平成１４年度調査】全体
今後、実用化（製品化）を見込んでいる分野

1	セキュリティマネジメント（30.4%）
2	ネットワークセキュリティ（26.1%）
2	セキュリティサービス関連（26.1%）
4	認証技術（23.9%）
5	不正侵入対策（19.6%）
6	暗号技術（15.2%）
7	ウイルス対策（2.2%）

【平成１５年度調査】全体
現在、実用化（製品化）されている分野

1	認証技術（33.0%）
2	暗号技術（26.4%）
2	セキュリティマネジメント（26.4%）
4	ネットワークセキュリティ（24.2%）
5	セキュリティサービス関連（18.7%）
6	不正侵入対策（9.9%）
7	ウイルス対策（7.7%）

【平成１５年度調査】全体
今後、実用化（製品化）を見込んでいる分野

1	ネットワークセキュリテ（28.6%）
2	認証技術（23.1%）
3	セキュリティサービス関連（22.0%）
3	セキュリティマネジメント（22.0%）
5	暗号技術（18.7%）
6	ウイルス対策（9.9%）
7	不正侵入対策（7.7%）

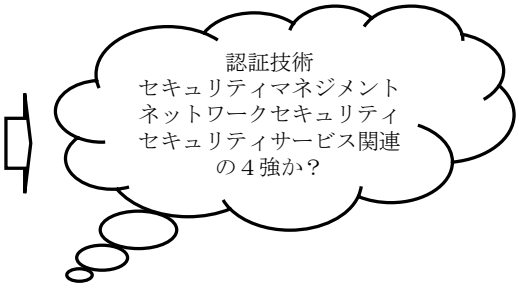
【本調査】全体
現在、実用化（製品化）されている分野

1	ネットワークセキュリティ（21.8%）
2	認証技術（20.8%）
2	セキュリティサービス関連（20.8%）
4	セキュリティマネジメント（18.8%）
5	暗号技術（15.8%）
6	不正侵入対策（13.9%）
7	ウイルス対策（12.9%）

【本調査】全体
今後、実用化（製品化）を見込んでいる分野

1	認証技術（18.8%）
2	セキュリティマネジメント（16.8%）
3	ネットワークセキュリティ（15.8%）
3	セキュリティサービス関連（15.8%）
5	暗号技術（7.9%）
5	不正侵入対策（7.9%）
7	ウイルス対策（5.0%）

【実用化（製品化）の今後の展望】
これまでの推移から



(4)現在取り組んでいる分野と今後取り組む分野の相関関係

現在取り組んでいる分野と、今後取り組む予定がある分野との相関を取ってみた。現在も今後も継続して取り組むと回答した部分が、次の表の太線で囲われた部分であるが、ほぼ50～60%程度の割合となっている。ここでは、現在取り組んでいる分野ごとに今後取り組む予定のある分野の上位三つを網掛けしてあるが、現在取り組んでいる分野によらず、今後取り組む予定がある分野に偏りが見られる。特徴的なのは、「認証技術」「ネットワークセキュリティ」「セキュリティマネジメント」に集中している。

この傾向は、現状の問題点を解決する方法論として認識されているテーマと符合している。

現在、取り組んでいる分野	今後、取り組む予定がある分野								
	暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	セキュリティサービス関連	その他	特に計画無し
暗号技術	60.71	57.14	42.86	35.71	50.00	28.57	39.29	14.29	10.71
認証技術	46.34	63.41	51.22	41.46	48.78	31.70	43.90	17.07	7.32
ネットワークセキュリティ	36.36	52.27	63.64	43.18	45.45	31.82	38.64	18.18	11.36
不正侵入対策	40.63	50.00	50.00	53.13	53.13	40.63	46.88	18.75	12.50
セキュリティマネジメント	38.24	47.06	47.06	41.18	55.88	26.47	50.00	14.71	11.76
ウイルス対策	38.46	50.00	53.85	50.00	50.00	46.15	42.31	11.54	15.38
セキュリティサービス関連	33.33	42.42	48.48	39.39	57.58	27.27	63.64	18.18	12.12
その他	33.33	50.00	41.67	33.33	25.00	25.00	25.00	75.00	8.33

次に、現在取り組んでいる分野と、今後最も力を入れていく分野の相関を取ってみた。これも、現在と今後で同じテーマで継続する部分を太字で囲ってあるが、『最も力を入れる』という条件をつけると、必ずしも現在の取り組みを継続するとは限らない「変化」が見えてくる。

特に顕著なのが、「ウイルス対策」と「不正侵入対策」である。ウイルス対策の次は、ネットワークセキュリティとセキュリティマネジメントに力点を移す傾向があり、不正侵入対策については、セキュリティマネジメントと認証技術が次のテーマになっているようであ

る。また、今後最も力を入れていく分野としては、認証技術とセキュリティマネジメントが多く選択されている。

この結果も、セキュリティ関係の動向の一般的な感覚と違和感がない。現在、問題点としてもたれているテーマの変遷が見えているといっても良いだろう。

現在、取り組んでいる分野	今後、最も力を入れていく分野									
	暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	セキュリティサービス関連	その他	特に計画無し	無回答
暗号技術	14.29	14.29	0.00	0.00	10.71	0.00	10.71	3.57	7.14	39.29
認証技術	9.76	19.51	7.32	0.00	14.63	9.76	9.76	4.88	2.44	31.71
ネットワークセキュリティ	4.55	13.64	13.64	0.00	11.36	0.00	9.09	6.82	6.82	34.09
不正侵入対策	3.13	12.50	3.13	3.13	18.75	0.00	6.25	6.25	6.25	40.63
セキュリティマネジメント	2.94	14.71	2.94	0.00	20.59	0.00	11.76	2.94	5.88	38.24
ウイルス対策	3.85	7.69	11.54	0.00	11.54	0.00	3.85	3.85	7.69	50.00
セキュリティサービス関連	3.03	9.09	3.03	0.00	15.15	0.00	21.21	6.06	3.03	39.39
その他	0.00	8.33	8.33	0.00	0.00	0.00	8.33	33.33	8.33	33.33

アクセス制御機能に関する技術の研究開発の今後の見通しについて、本調査結果、並びに過去の調査結果との比較から、アクセス制御機能に関する技術の研究開発および実用化（製品化）において、（今回、回答肢として設定した）７分野では、下記が重点になると思われる。

- 認証技術
- ネットワークセキュリティ
- セキュリティマネジメント

とりわけ、認証技術およびセキュリティマネジメントが次世代の IT 基盤を先導する形で展開していくことが予想される。

［引用］

平成１４年度「アクセス制御機能に関する技術研究開発の状況等に関する調査」報告書
http://www.npa.go.jp/cyber/research/h14/accesscontrol-2/index.htm
平成１５年度「アクセス制御機能に関する技術研究開発の状況等に関する調査」報告書
http://www.npa.go.jp/cyber/research/h15/image/H16research.pdf

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。

⑴ 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、クライアントなど大きな括りの視点で見る。

⑵ 何から保護するか？
- 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。

⑶ 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。

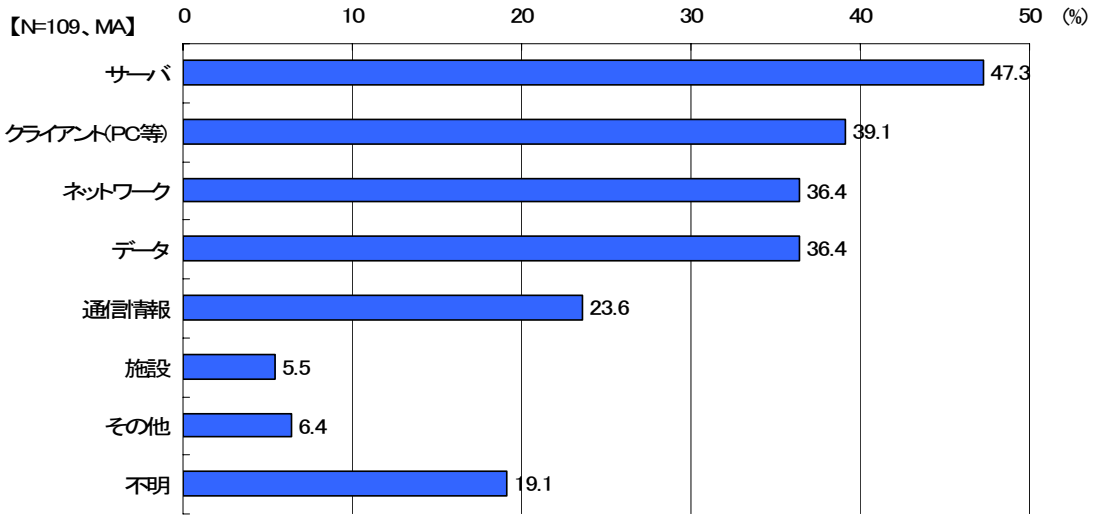
⑷ どのようなサービスか？
- サービスの場合、どのような内容か、という観点から見た分類。

(1)何を守るか？

①実用化（製品化）されているもの

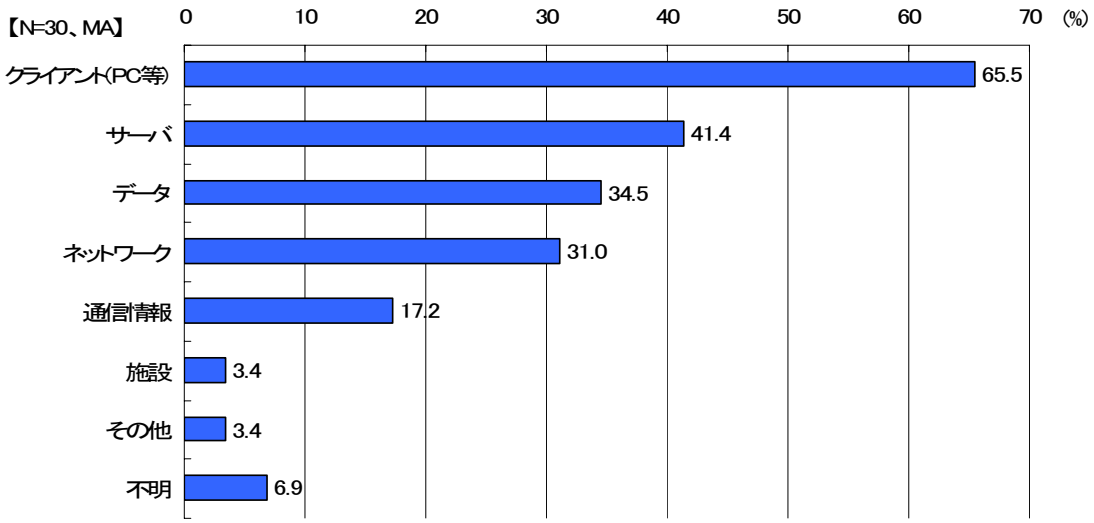
「何を守るか」という視点で実用化されている分野を見ると次の図のようになる。サーバを守るものが約 5 割と一番多いが、クライアント、ネットワーク、データを守るものも約 4 割とかなり多数を占めている。図の上位 5 つは、ネットワーク、コンピュータ、データ通信という、ネットワークセキュリティに直接かかわる部分である、この分野の研究開発が成熟し製品化が進んでいるというのは頷ける。

一方で、施設は数こそ約 5%と少ないが、最近の ISMS 取得や管理強化を背景に、IC カードやバイオメトリクス関連など、認証と施設の入退出設備とが関連した技術・サービスが見られる。


【N=109、MA】
0
10
20
30
40
50
(%)
サーバ
47.3
クライアント(PC等)
39.1
ネットワーク
36.4
データ
36.4
通信情報
23.6
施設
5.5
その他
6.4
不明
19.1

②研究開発中のもの

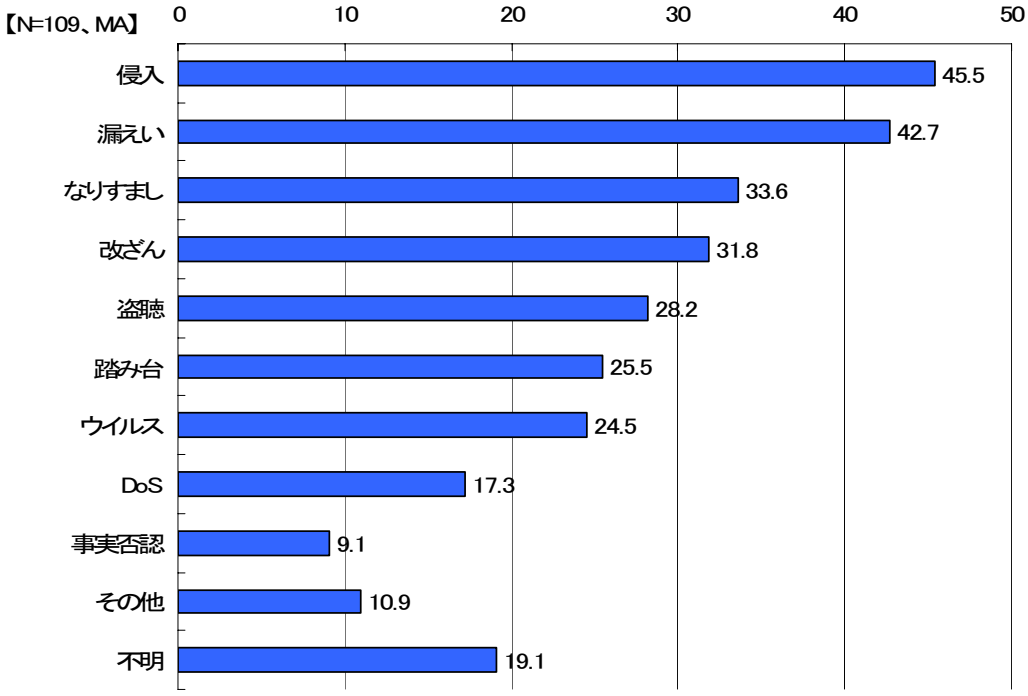
研究開発中のものでは、クライアント(PC)にかかわるものが 65.5%と圧倒的に多い。これは、変化の早いパソコンが、商品開発の対象として投資効果があるということでもあるのだろう。また、モバイルパソコンの盗難や紛失について、社会的な話題ともなっているので、需要も多いことが考えられる。他の部分は、実用化（製品化）されているものと大きな差はない。



(2)何から保護するか？

①実用化（製品化）されているもの

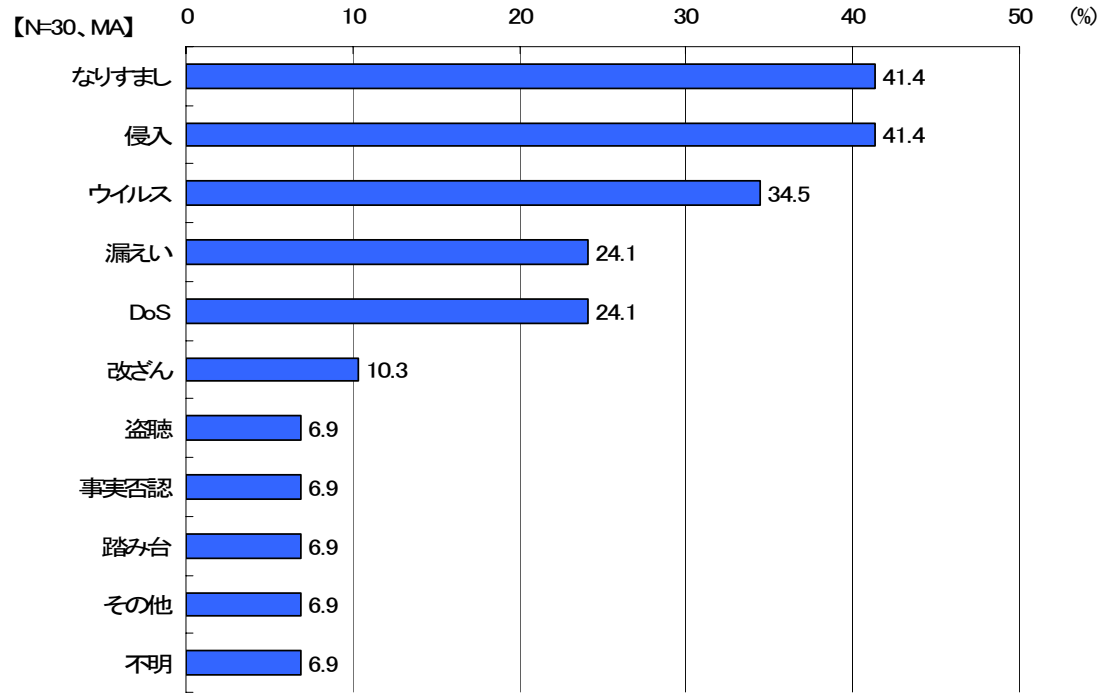
「侵入」と「漏えい」が約 45%と多いのは、ファイアウォール系の製品が主流であることによるのだろう。それ以外はそこそこ満遍なく実用化（製品化）の段階に来ているようである。事実否認が少ないが、これは暗号メールや PKI（公開鍵暗号基盤）などが実現されるに伴い、重要な位置付けになってくると思われる。



②研究開発中のもの

研究中のターゲットとしては、「なりすまし」と「侵入」が各々40%を超える多数を占めており、「ウイルス」が 35%弱と続いている。それ以外には、「漏えい」と「DoS」が各々24%強と多いが、「なりすまし」はフィッシング、迷惑メールなどが大きな社会問題となっている中、関心が高く、認証システムで対応することになると思われるが、まだ試行錯誤の段階であると考えられる。

研究開発中のものの特徴は、DoS とウイルスの比率が、実用化されているものに比べ大きいことである。DoS(サービス妨害攻撃)は、サーバを事実上利用不可能にする可能性があり、今後のサイバーテロ関連でも注目されている。ウイルス関係も、ワーム、スパイウエア等が社会的な問題となっていることから、今後ますます重要性が高まるものと考えられる。

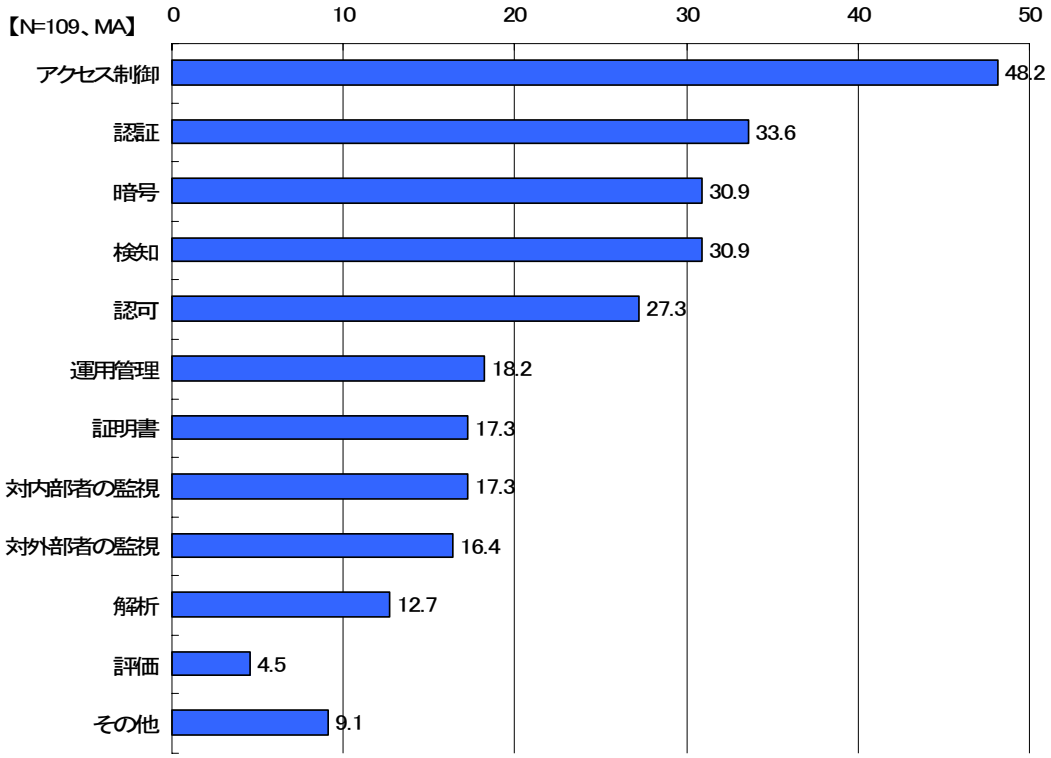


(3)どのような機能を持つか？

①実用化（製品化）されているもの

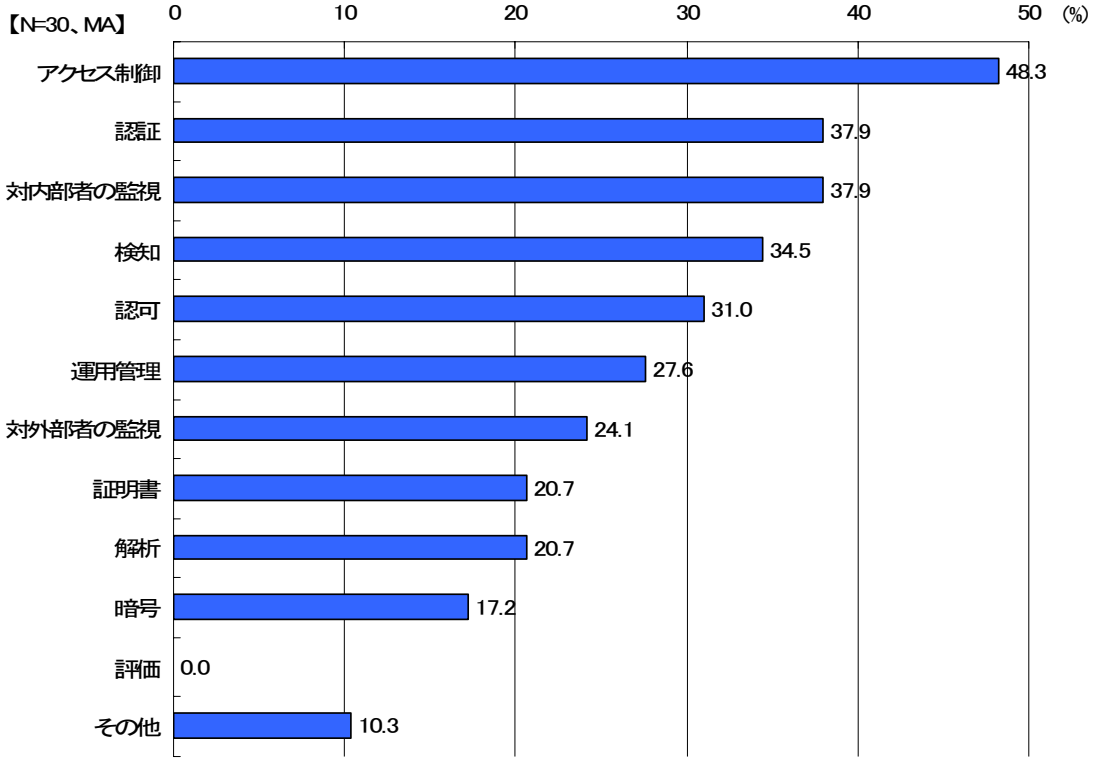
実用化（製品化）されている機能で多いものは「アクセス制御」で約半数を占めている。続いて、「認証」「暗号」「検知」「認可」などが約 30%前後で続いており、個人や装置の認証、転送データの秘匿化、インシデントの検知が実用化されていることが伺われる。

内部者と外部者の監視は、約 20%弱でほぼ同じレベルとなっており、どちらも同程度に実用化されている。



②研究開発中のもの

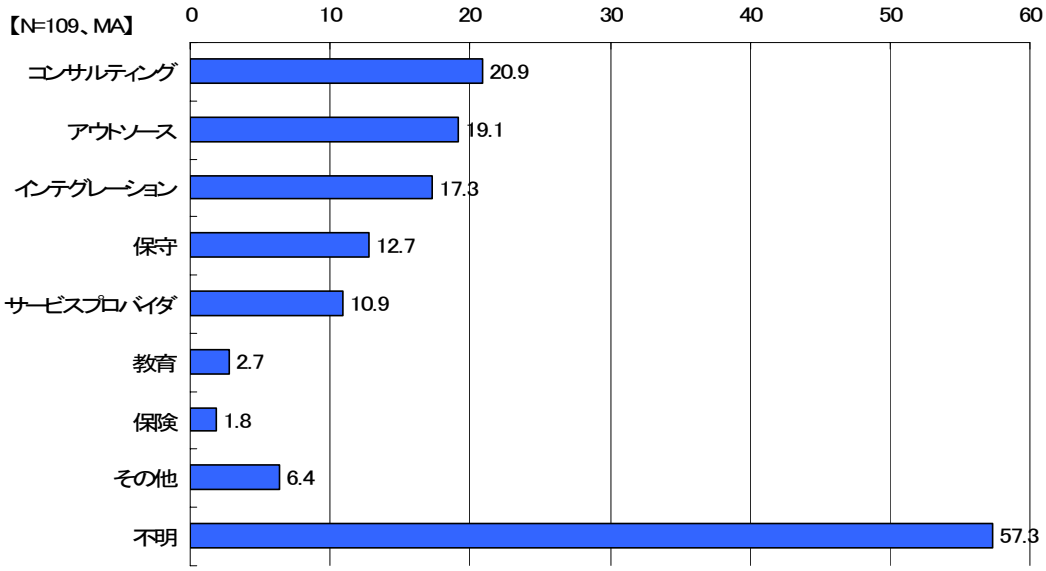
研究開発でも「アクセス制御」が約半数弱となっており、全体の傾向はあまり変わらないといえる。ただ若干特徴的なのは、「対内部者の監視」が約 4 割弱とかなり大きな割合を占めていることがある。これは、最近の報道されている情報漏えい関係の事例も、多くが内部の人間が関係しているので、これらに対応するための研究開発の需要と意欲が大きいものと思われる。監視にはバイオメトリクスや認証システムなどのほかに、監視カメラや運用手順、管理基準、リスク管理など、ネットワークに係わるアクセス制御などの IT 技術以外の論点も大きな比重を占めていると思われる。



(4)どのようなサービスか？

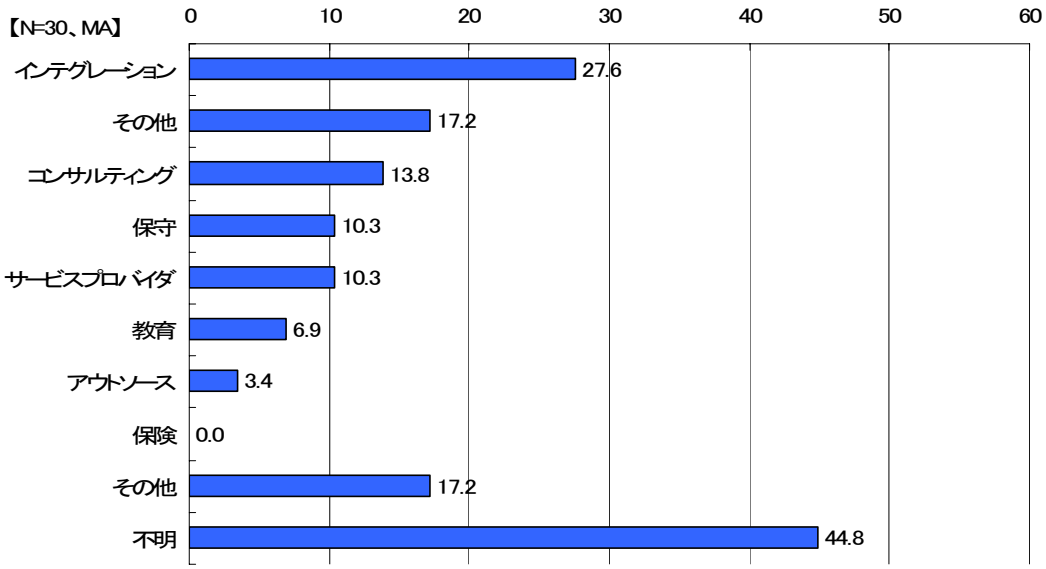
①実用化（製品化）されているもの

サービスについての回答は空欄が多く、有効回答数は少なかったものの、「コンサルティング」「アウトソース」「インテクレーション」が約 2 割を占めている。
「保険」は少ないが、アンケート対象企業に保険業務を行っている企業が少なかったためと考えられる。



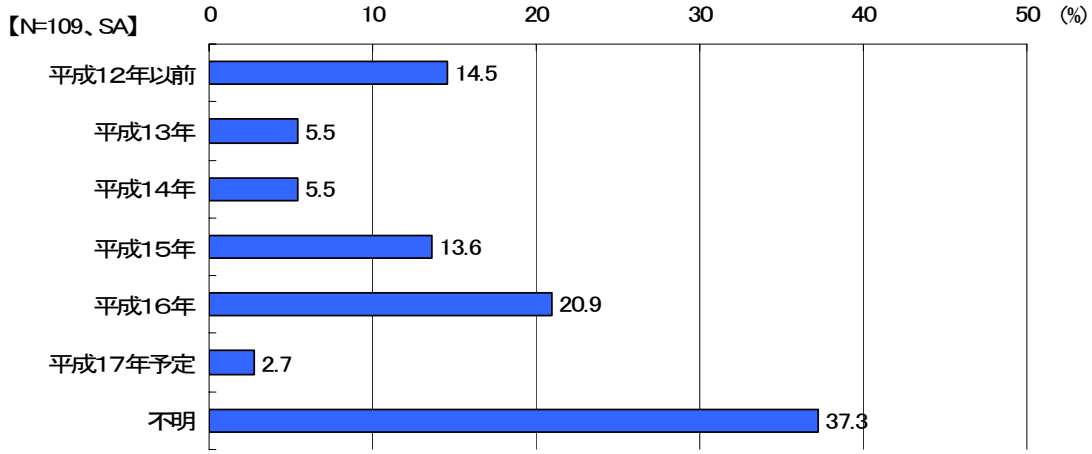
②研究開発中のもの

サービスに対する研究開発という位置づけがあまり一般的ではなかったせいか、製品と同様に回答数は少ないが、概ね同じ傾向を示しているといえるだろう。その中で「インテグレーション」が約 3 割弱と多数派となっている。サービスの研究開発という意味では、既存の製品やサービス群を組み合わせて、顧客満足度を上げるようなサービスを提供するという意味での「インテグレーション」が重視されていると思われる。



(5)発売時期の分布

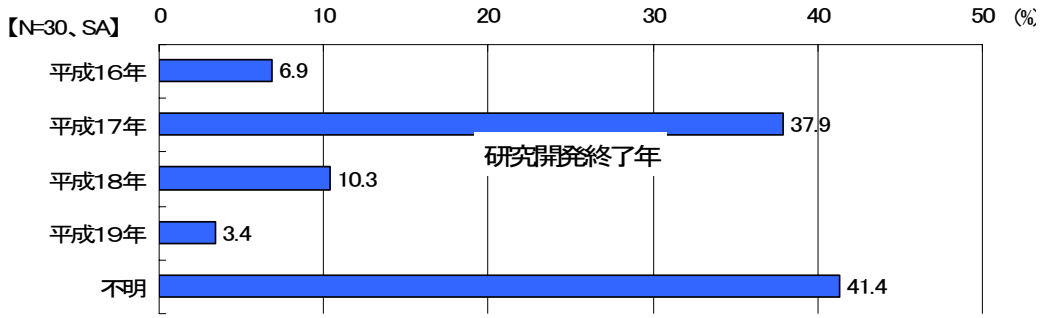
実用化され発売する時期を聞いたところ、「不明」が約 4 割弱と一番多かったが、時期が決まっているものは、2004 年(平成 16 年)が約 2 割強と最多数を占めた。アンケートを取った年に発売されたものが多いということだが、過去(4 年以上前)に発売されたものも引き続き販売されていることも伺える。セキュリティ関係のシステムは、バージョンアップを伴うにしろ、数年のライフサイクルで終わるものと、長い寿命を持つものに 2 分化される傾向があるようである。

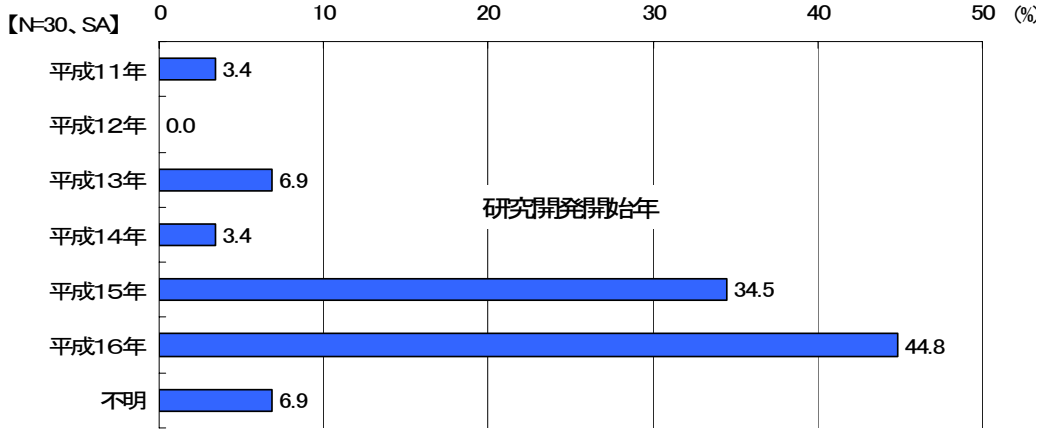


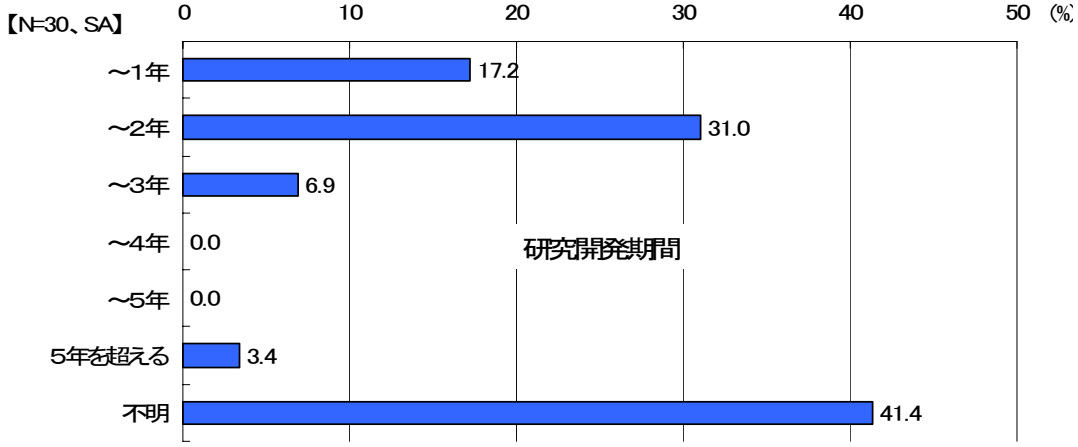
(6)

(7)研究開発時期の分布

(1)研究開発期間の目処としては、調査年の翌年(平成 17 年)中に終了し、実用化したいというものが多いようである。その一方で特に開発時期を区切っていないもの多く、基礎開発を継続的に続けていると見られる。







2.2 聞き取り調査結果

(1)ネットワークを守る

■DNS クエリによる DDoS 攻撃検知ならびに防御

研究開発団体：熊本大学総合情報基盤センター

1. 研究開発の目的・ねらい

DNS 解決パケットが送りつけられる分散型サービス妨害攻撃(DDoS)に対し、DNS 未解決型攻撃を感知し、自動的に阻止するシステム(IPS)を開発する。

2. 研究開発に至った経緯

熊本大学のトップドメイン DNS サーバが大量の DNS 解決パケットを送りつけられる DDoS 攻撃を受けた際に、DNS サーバの syslog を統計的に解析したところ、次のような結果を得た。

(1) DNS 解決 DDoS 攻撃パケットは、主に逆引(PTR)レコードで構成されている。
(2) その PTR レコードで解決する IP アドレスは、主として熊本大学の未使用 IP アドレスである。

このことから、未使用 IP アドレスの PTR レコードを監視すれば、DNS 解決型 DDoS 攻撃を検知することが可能となる。

3. 研究開発の内容（特徴）

DNS サーバを安全に保つため方法のひとつとして、侵入検知システム(IDS)を組み込むことがある。IDS は、正しくない状態を検出するタイプの MID (misuse intrusion detection) と、攻撃データをデータベースに検索して例外操作を検出するタイプの AID (anomaly intrusion detection)に分類できる。最近の IDS は両方の機能を兼ね備えているものが多く、有用なアラートを報告してくるが、あまりに多くのアラートが生成されるので、実時間で解析することが難しい。

このため、新しい MID/AID ハイブリッドタイプで、DNS サーバへの攻撃を予測するシステムの実証実験を行っている。これは、DNS サーバと DNS クライアント間での DNS クエリーパケットのトラフィックを監視するものである。

最近、熊本大学のトップ DNS サーバが DNS クエリーベースの DDoS (DNS-DDoS: DNS query-based distributed denial-of-service) にさらされた際の研究を元に、DNS-DDoS をどのように検出し、どのように防止するかについて述べる。実験評価を行ったシステムの概要イメージを図 1 に示す。

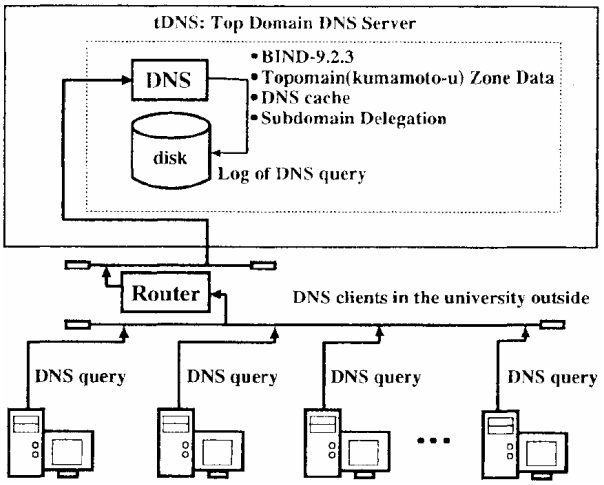


図 1：実験評価システムの構成概要

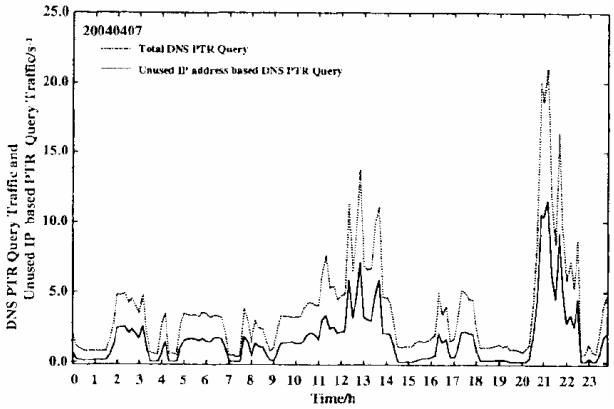


図 2：トップドメイン DNS サーバと DNS クライアント間の DNS クエリ PTR トラフィック(2004 年 4 月 7 日観測)

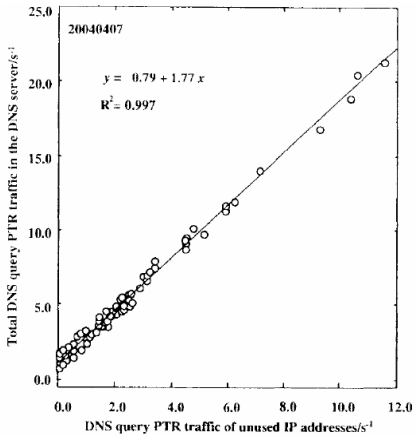


図 3：全 DNS クエリ PTR(逆引)と未使用 IP アドレスに対する PTR トラフィックの相関関係(2004 年 4 月 7 日観測)

図 2、図 3 に実際に測定したデータを示す。これを見ると、全体の DNS 逆引きパケットと、未使用アドレスが指定されている DNS 逆引きパケットの比率は、ほぼ一定となっている。これから熊本大学では、不正な DNS 逆引きのトラフィックは、未使用 IP アドレスを持つ逆引き DNS トラフィックと相関を持っていることがわかった。

熊本大学は、逆引き DNS クエリを使った DDoS 攻撃を検出し阻止するための PTRDPS を開発した。このシステムは、逆引きパケットをキャプチャすることと、逆引きレコードを解釈する “arpa”、DDoS 攻撃を検出するエンジン “ptrscan”、DDoS 攻撃から防御する “pfd.pl” などから成る。検出システムは、Perl スクリプトの “ptrscan” が “ptrds.pl” から 10 秒毎に実行される。

PTRDPS を我々のトップドメイン DNS (tDNS)サーバに実装した。この結果、実装前に比べて逆引き DNS クエリのトラフィックは、図 4 に見られるように劇的に穏やかになった。

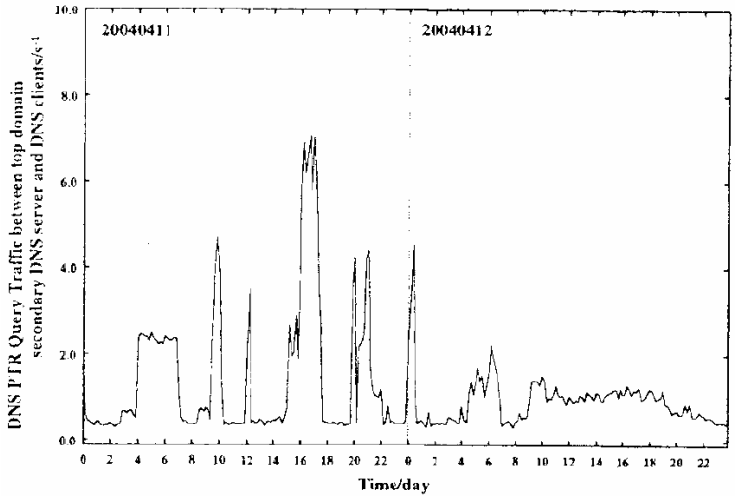


図 4：左側(4/11)のシステム稼動前と右側(4/12)のシステム稼動後の比較

4. 研究開発の課題

トップドメイン DNS (tDNS)のシステムログを調べると、外部からの DDoS 攻撃として、不正な逆引き DNS パケットが多数記録されている。今後の課題として、DNS や E-mail サーバに対する DDoS 攻撃の更に詳細な情報を調査研究することがあげられる。

5. 導入事例・利用イメージ

DDoS アタックに対して、リアルタイムに自動検出、自動ブロックを行う。

6. 研究開発の到達目標

DDoS の動作を解析し、実用的なシステムとして利用できることを目指している。

連絡先
組織名：熊本大学
部署名：総合情報メディアセンター
住所：〒860-8555 熊本県熊本市黒髪２－３９－１

■MTA による SPAM 対策システム

研究開発団体：中京大学情報科学部

1. 研究開発の目的・ねらい

MTA(メールサーバ)で spam を受信拒否するシステムを開発、普及することにより、spam によって滅びようとしているインターネットの延命を図る。

2. 研究開発に至った経緯

spam と不適切な MTA 運用によるバックスキャッタにより、インターネットは崩壊の危機に瀕している。spam とバックスキャッタを排除するためには、MTA において spam セッションを判別して排除する必要がある。当初、NPO 東海インターネット協議会のサーバをフィールドとして研究を開始し、現在、中京大学と株式会社リフレクションの共同研究として研究開発を進めている。

3. 研究開発の内容（特徴）

従来の spam 対策はメールを受信した後に判定を行うものが大半であった。それでは spam がリソースに掛ける負荷は減るどころか増加してしまう。本研究では、SMTP セッションを選別して spam を排除することを特徴としている。spam は RFC2821 を遵守していないことを利用して、90%程度の spam を受信拒否することができる。これによりネットワーク負荷、サーバ負荷ともに最小化することができる。

特に最近の研究では TCP のハンドシェイクの途中で spam を拒否することを目指しており、世界最小コストの spam 対策が実現できる見通しである。

なお、統計的な「判定」を行わないため、false positive がない。

4. 研究開発の課題

大量のセッションへの対応
RFC2821 に従わないプロダクトへの対応（ホワイトリスト）
RFC2821 に従う spam が増えたときには別な対策が必要となる。

5. 導入事例・利用イメージ

現用の MTA の置き換え。または、現用 MTA の手前（インターネット側）にリレーサーバとして設置する。

すでに第一世代のシステムは、東海インターネット協議会、株式会社リフレクション、

某学会において実稼動中であり、80 から 90%以上の spam を false positive なしに排除できている。

6. 研究開発の到達目標

spam の撲滅とインターネットの延命

連絡先
組織名：　中京大学
部署名：　情報科学部情報科学科
担当者：　鈴木常彦
住所：〒470-0393　豊田市貝津町床立 101
E-mail：tss@sccs.chukyo-u.ac.jp

(2)サーバを守る

■Solaris 10

研究開発団体：サン・マイクロシステムズ(株)

1. 研究開発の目的・ねらい

Solaris 10 は、最近話題に上ることの多いセキュア OS の機能を標準で取り込み、商用 OS として様々なアクセス制御機能を実装している。

2. 研究開発に至った経緯

近年のインターネットは、企業がサービスを提供する方法を劇的に変化させた。継続的なサービスを提供する能力を確保するために、多くのサーバ群を水平的かつ垂直的にスケールすることが望まれている。特にセキュリティの確保は重要である。このために、セキュア OS あるいはトラステッド OS と呼ばれるアクセス制御方式が一部で使われていたが、これ等を標準 OS として実装し提供するに至った。

3. 研究開発の内容（特徴）

Solaris 10 では、いわゆる「セキュア OS」と呼ばれる機能が追加されている。この他、暗号化フレームワークが再設計され、暗号化デバイスや暗号や認証のソフトウェアなどの組み込みが容易になった。主なものを簡単に説明する。

- **Process Right Management**
  Process Rights Management コンポーネントは、どのユーザをどのプロセスに対し、何時、どのような権限を与えるのか詳細な制御を可能にする。この機能は Solaris 8 以降の Role-Based Access Control(RBAC)と融合されている。
  従来のオペレーティングシステムでは、スーパーユーザになれるユーザ（管理者）全員にスーパーユーザ権限が与えられることになり、管理者に必要以上の権限が与えられているが、それに対して RBAC では管理のための一連の作業を担うユーザに制限付きの管理権限を割り当てることが可能になる。これまでの RBAC に Process Right Management が融合することにより、最小特権のポリシーに基づき、スーパーユーザをシステムから完全に排除し、その代わりとしてユーザやプロセスに対して必要最小限の権限を許可することが可能となる。
- **Solaris コンテナ**
  Solaris コンテナは、サービスレベルに応じて優先順位を持たせたリソースの動的な提供を行う。各アプリケーションは独自の環境が提供されるため、事実上他のアプリケーションからの影響を受けることがなく、不正なアクセスや侵入を防ぐことができる。
- **DTrace**
  DTrace は、包括的なトレース機能フレームワークである。パフォーマンスへほとんど影響を与えずに、実稼動しているシステム上でアプリケーションのパフォーマンス・チューニングとトラブルシュートが行える。
- **Self-Healing（予測的自己修復機能）**

予測的自己修復機能は、どのようなハードウェア／アプリケーション障害も自動的に特定し、診断／分離／修復できる機能である。ソフトウェアやハードウェア障害等が発生した場合でも、継続してサービスを提供することが可能となる。

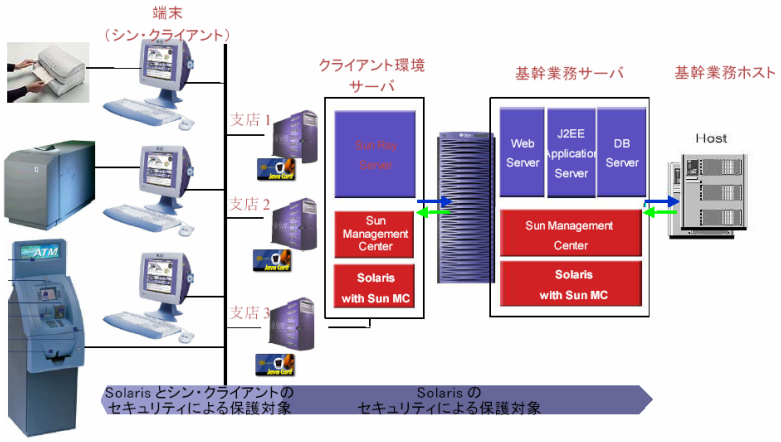
- **Solaris ZFS**
  Solaris ZFS(ゼタバイト・ファイルシステム)は、多くの管理タスクを自動化することでファイルシステムの管理や保守を容易にする。仮想化されたストレージ・プールを利用し、ドライブを追加するだけでファイルシステムの拡張が行える。

4. 研究開発の課題

（公開を控えさせていただきます）

5. 導入事例・利用イメージ

銀行で利用される事例として、Solaris10 のセキュリティ機能を基盤として、IC カードによる認証基盤、シン・クライアントによる端末でのセキュリティ、ミドルウェアレベルおよびアプリケーションレベルのセキュリティを確立し、ミッション・クリティカルなクラスのセキュリティ環境を実現できる。



6. 研究開発の到達目標

サービス・レベルを向上させ、サービス・コストとリスクを押さえるように企業を支援することである。スケーラビリティ、可用性、管理性、そしてセキュリティに優れたシステムを構築するプラットフォームとして使用されることにある。

連絡先
組織名：サン・マイクロシステムズ株式会社
部署名：e-Japan 営業開発本部
担当者：岡野　直樹
住所：〒100-6160 東京都千代田区永田町 2-11-1 山王パークタワー12F
電話：03-4232-2701
E-mail：Naoki.Okano@Sun.COM
URL：http://jp.sun.com/

(3)クライアント(PC)を守る

■Sun Java System Access Manager

研究開発団体：サン・マイクロシステムズ(株)

1. 研究開発の目的・ねらい

Sun Java System Access Manager は、企業の内側だけではなく、B2B (business-to-business)の企業 Web アプリケーションで、オープンな認証機構とポリシーベースの承認を実現する。

2. 研究開発に至った経緯

2001 年 12 月に 6 社の企業により、インターネットを通じた複数のコミュニティにおいて、アイデンティティ管理の連携を実現するために、オープンで相互運用が可能な標準およびガイドラインの策定を目標として、Liberty Alliance が設立された。これはインターネットを通じたビジネスの課題を解決するために、グローバルかつ業界の垣根を越えて進められている標準策定の取り組みであり、現在、世界 150 社を超える大手企業が参加している。

Liberty 仕様のフェーズ I は 2002 年に公開され、ドメイン間のアカウントリンクおよび連携の基盤を作った。Liberty 仕様のフェーズ II は 2003 年 11 月に公開され、この中にはアイデンティティを基準にした Web サービス配信のためのフレームワークが含まれている。

3. 研究開発の内容（特徴）

- **シングルサインオン**
  セキュリティを向上させるために認証条件を適切に適用する。複数のアプリケーションやプラットフォーム、そしてインターネット・ドメインにおけるシングルサインオンを可能にし、ユーザビリティを向上する。
- **一元化された認証サービス**
  一貫性のあるセキュリティポリシーの適用を実現してセキュリティを向上させ、アプリケーションの開発と管理に必要なコストを削減する。
- **アイデンティティの共有サービス**
  Liberty Alliance のフェーズ 2 である ID-WSF と SAML 1.1 の仕様への準拠により、枠組みを超えたビジネス・ネットワークでの アイデンティティの共有を実現するとともに、法制度へのコンプライアンスと、HIPAA／GLBA／European Privacy Directive など世界中の主要なプライバシー・ポリシーや規制に 対応する強力なフレームワークを提供する。
- **J2EE アーキテクチャと包括的な API 群**
  高いレベルの統合とカスタマイズが可能な、オープンで仕様に則った設計を採用し、コストの削減と開発期間の短縮を実現する。
- **エンタープライズクラスの拡張性と信頼性**

複数の負荷分散ポリシー・サーバ／ポリシー・エージェント／ディレクトリ・インスタンスが、高い可用性とフェイルオーバー機能を提供し、 単一機能障害を排除することで、ミッションクリティカルなアプリケーションの信頼性と拡張性を向上する。

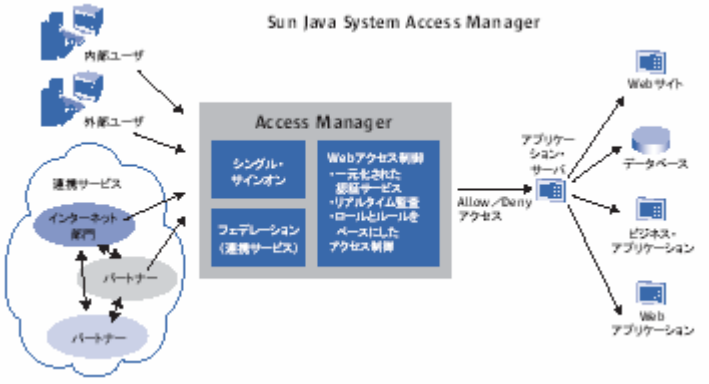
- **リアルタイムな監査**
  認証の試み／承認／変更内容に関する最新情報の監査を可能にし、情報へのアクセスに関する重要な情報を容易に確認できることで セキュリティを向上する。

4. 研究開発の課題

（公開を控えさせていただきます）

5. 導入事例・利用イメージ

Web サービスにおけるシングルサインオン関連の仕様を定めた Liberty Alliance のフェーズ 2 である ID-WSF（Liberty Identity Web Services Framework）と、SAML（Security Assertion Markup Language）1.1 仕様に準拠し、サービスの統合化と、複数のアプリケーションに対するセキュアなシングルサインオン環境を提供する。



6. 研究開発の到達目標

Sun Java System の目標は、企業が必要とするソフトウェアの購入／開発／管理をシンプルにし、ひとつのソフトウエアを、ネットワーク上のどのようなパソコンやデバイスでも実行できることである。

連絡先
組織名：サン・マイクロシステムズ株式会社
部署名：e-Japan 営業開発本部
担当者：岡野　直樹
住所：〒100-6160 東京都千代田区永田町 2-11-1 山王パークタワー12F
電話：03-4232-2701
E-mail：Naoki.Okano@Sun.COM
URL：http://jp.sun.com/

(4)クライアント(PC 等)を守る

■新幹系統

研究開発団体：インテリジェントディスク(株)

1. 研究開発の目的・ねらい

１）ネットワークに接続する個人や団体の情報をネット犯罪から保護する目的で、個々の情報を、ＨＤＤとは異なるバスに接続されＩＣチップ等の電子回路を有する光ディスクに保存し、当該電子回路が能動的且つ自律的に生態認証を含む認証並びにセキュリティ管理を行う。さらに、ネットワーク管理センター側のサーバが生成するワンタイムパスワードとは異なるアルゴリズムに基づくワンタイムパスワードを二元的に生成する事により、データの可搬性を含むユビキタス機能と高度なセキュリティ機能を併せ持つ、ネットワークコミュニティを構築するためのデバイスを開発する。

２）上述のデバイスとＰ２Ｐセッション管理技術を融合させることにより、匿名性を排除した安心且つ安全なネットワークコミュニティを構築する為のプラットフォームを開発する。

2. 研究開発に至った経緯

１）ＰＣに組み込まれたＨＤＤなどのメモリーデバイスとは異なるバスで接続された光ディスクの裏面に CPU 等の電子回路を搭載し、ディスクを交換するだけで容易にセキュリティアルゴリズムを多様化する事が可能なインテリジェンスを有する記憶媒体ができるのでないかということで特許を出願した。

２）RFID を始め周辺装置の小型軽量化が進展し、１）の内容を実現できる時代がやってきた。

３）当社が開発した RFID(CPU)付き光ディスク及び専用ドライブと、東京電力が開発した P2P セッション管理技術を融合する事により、匿名性を排除した安心且つ安全なネットワークコミュニティを構築する為のプラットフォームを実現できる事が分かった。

3. 研究開発の内容（特徴）

１）ＲＦＩＤ（無線自動認識システム）対応のＩＣチップと光ディスクを一体化した知能ディスクの開発及び生体認証から起動されるＲＦＩＤのリーダ／ライタ付光ディスクドライブの開発

２）Ｐ２Ｐによるネットワークに対応したシステムソフトの開発

4. 研究開発の課題

１）個々のユーザのコンテンツ利用状況に合わせて、暗号アルゴリズムやコード及びセキュリティシステムをカスタマイズする為の手法の開発

２）利便性と安全性を兼ね備えたネットワーク上でのコミュニティ形成手法の開発

5. 導入事例・利用イメージ

１）生体認証を行うと同時に、ＩＣチップに、カスタマイズされた暗号アルゴリズム、暗号コードを搭載することにより、ローカライズされたセキュリティシステムが実現できるので、個人や団体の情報をネット犯罪から守ることができる。

２）管理センターおよび個人間では、利用するたびにＩＤやパスワードを人が介入することなく自動的且つ２元的に更新できるので、利便性が高くなると同時になりすましの問題が発生しない。

6. 研究開発の到達目標

匿名性を排除した安心且つ安全なネットワークコミュニティを構築する為、各種ＯＳに対応したネットワーク及び端末機器を開発し、デファクトスタンダード化する。

連絡先
組織名：インテリジェントディスク株式会社
部署名：開発本部
担当者：刈本博保
住所：〒222-0033
電話：045-470-5200
E-mail：karimoto@intelligentdisc.com
URL：http://www.intelligentdisc.com

(5)通信情報を守る

■秘文

研究開発団体：日立ソフトウェアエンジニアリング(株)

1. 研究開発の目的・ねらい

「秘文」シリーズでは、情報漏洩防止の為の情報セキュリティシステムの導入から、運用、監視、見直しまでの、トータルセキュリティを実現する。

2. 研究開発に至った経緯

企業の情報漏洩が相次いで発覚し､企業内での情報管理体制の更なる強化が急務となっており、また２００５年４月には個人情報保護法が完全施行される。

「秘文」シリーズでは、こうした情報漏洩防止対策に早い時点から着目し、１９９９年から「持出し制御」「暗号化」「アクセス制御」を中心にしたセキュリティシステム「秘文」の開発を行った。

3. 研究開発の内容（特徴）

「秘文」は､「持出し制御」「暗号化」「アクセス制御」の３つの機能を中心に、情報の「機密性」「安全性」「可用性」を実現している。

①クライアントＰＣから外部へ持ち出させない

ＦＤ，ＭＯ，ＵＳＢメディアによる持ち出しや印刷を制御する。持出し権限は管理者がユーザごとに設定し、不正な持ち出しを防止する。

②暗号化によって持ち出しても漏洩させない

クライアントＰＣのドライブやメディアに保存するデータを暗号化する。暗号化よって盗難や紛失時の情報漏洩を防止する。

③サーバへのアクセス制御で守る

ファイルサーバ上に共有機密フォルダとして共有データを暗号化する。アクセス権限はフォルダ単位設定し、グループやプロジェクトで共有する機密情報の漏洩を防止する。

4. 研究開発の課題

社内における情報漏えい防止については、トータル的にカバーできるようになってきたが、いったん社外に持ち出したあとの 2 次利用の制限という課題がある。

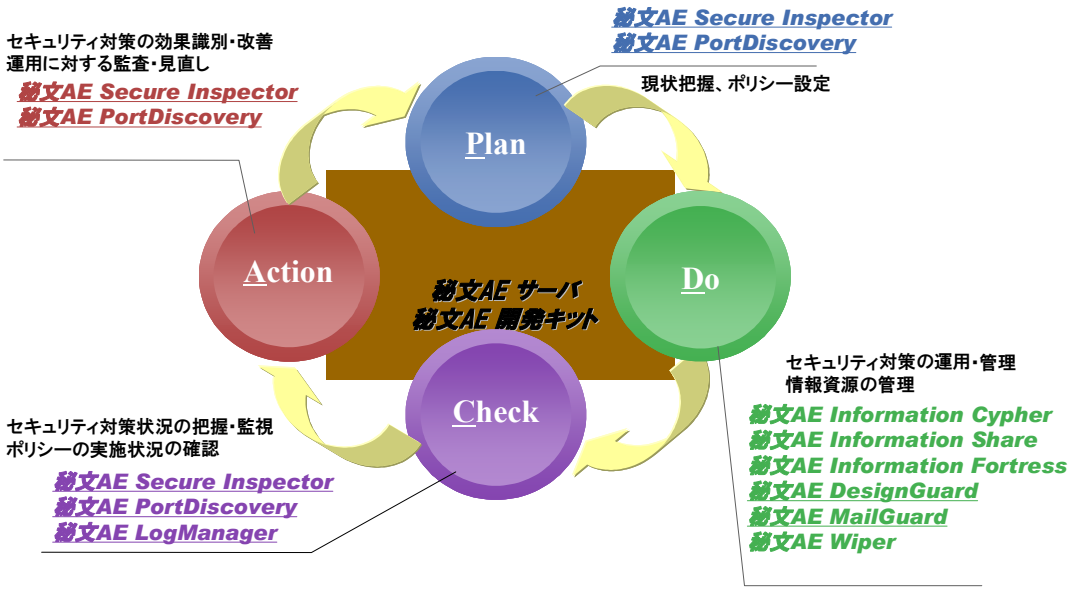
つまり､秘文が導入されてない企業との取引において相手に渡した後のデータの保証がない。たとえば､設計図を外注先に渡しても外注先から漏れないという保障ができない。この 2 次利用のファイルコントロールが現状の課題である。

5. 導入事例・利用イメージ

「秘文」シリーズは、現在金融機関や公共団体を中心に約６００社、５０万ライセンスの導入実績がある。さらに今年度中には１００万ライセンスの導入を目指している。

6. 研究開発の到達目標

相次ぐ企業の情報漏洩や２００５年 4 月の個人情報保護法の完全施行へ向け、トータルな情報漏洩防止対策の必要性が高まっている。ピンポイントになりがちな情報漏洩対策をトータルセキュリティとして実現する為に、ＩＳＭＳのＰＤＣＡマネージメントサイクルに基づいて、セキュリティシステムの導入から、運用、監視、見直しまでを行うシステムの開発を行っていく。



連絡先
組織名：日立ソフトウェアエンジニアリング(株)
部署名：ソリューション企画本部
担当者：馬場　章爾
住所:〒140-0002 東京都品川区東品川 4-12-7
電話：03-5780-6186
E-mail：baba@hitachisoft.jp
URL：http://hitachisoft.jp/

(6)データを守る

■情報セキュリティポリシー遵守管理システム Policy Guardian

研究開発団体：富士通関西中部ネットテック(株)

1. 研究開発の目的・ねらい

外部からの侵入よる情報漏えいは、様々なセキュリティシステムにより防御されてきたが、最近のインシデント事例を見ると、組織内部の者による故意あるいは誤操作による情報漏えいが増加し、情報セキュリティポリシー策定による運用対策など情報資産利用者の意識向上が急務となってきている。

当システムは、組織内の情報資産利用者に対して、強制的なアクセス制限をかけるのではなく、効率的かつ確実に情報セキュリティポリシーを浸透させ、遵守させることによりセキュリティを確保することを目的とする。

2. 研究開発に至った経緯

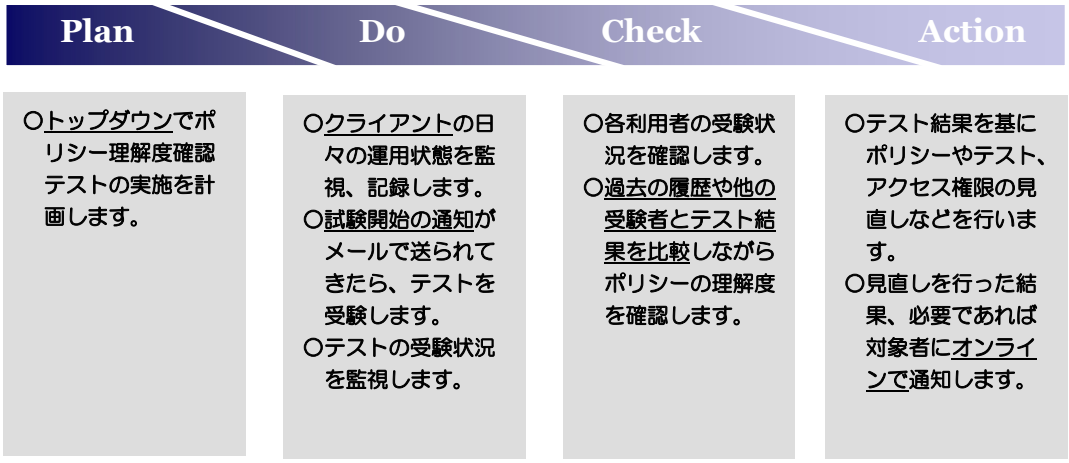
我々のキービジネスの一つとして、数多くの企業や自治体向けの情報セキュリティポリシー策定支援に取り組んできた。この経験から、策定後の運用に不可欠な要素として啓蒙教育の重要性を痛切に感じ、これをシステム化するに至った。

3. 研究開発の内容（特徴）

本システムは、セキュリティマネジメントの基本であるＰＤＣＡサイクルに従って運用されることをコンセプトとしている。まず、端末利用者に対するリスク許容値を決定する。本システムは、全ての端末利用者のネットワーク利用状況を監視し、個人単位に集計を行い、リスク許容値との比較分析データを出力する。この結果により、理解度が不足していると思われるカテゴリについて、情報セキュリティポリシー理解度を確認するテストを生成し、情報資産利用者に対して実施する。このテスト結果を含めた統計情報を基に、組織全体として情報セキュリティポリシーがどれだけ定着しているかを把握することができる。また、常に情報セキュリティポリシーから逸脱したネットワークの利用実態が監視されていることから、不正利用者に対する抑止効果も期待できる。

本システムを導入することで、情報セキュリティポリシーの浸透度が向上し、さらに状況を可視化することで、次に打つべき対策を早期に検討することができる。

製品では、(1)テスト問題作成，(2)テスト受験，(3)テスト結果の統計表示及びファイル出力，(4)管理者や利用者への各種通知，(5)メール発信記録収集，(6)URL アクセス記録収集といった機能を実装している。今後、ネットワーク利用状況の統計表示機能などを実装し、機能を充実させていく予定である。



4. 研究開発の課題

ネットワーク上を流れる情報には、様々な種類があり、それぞれ異なる手順や形式でやりとりされている。これらの情報を解析し、ネットワーク利用状況を分析するには、それぞれ専用の分析システムを開発しなければならない。

一般に、ネットワーク上を流れる情報を収集および分析するには、膨大な情報を処理するために高性能な専用のシステムを導入することが多い。最近は、Ｐ２Ｐソフトなどでもネットワーク上の通信そのものが暗号化され、ネットワーク利用状況の分析には高度な技術と高性能なシステムが要求される。利用者毎の利用状況を把握するためには、いかにして専用のシステムを用いずに情報の収集と分析を行うかが大きな課題である。

5. 導入事例・利用イメージ

電子商取引や会員向け WEB サービス、e-Japan など、ネットワーク上で各種情報資産を扱う様々な企業や自治体などで利用できる。特に、顧客情報や個人情報、他社秘密情報を扱う部門では、情報セキュリティポリシーの遵守が必須であり、このような部門でこそ、本システムが本領を発揮すると考えている。

本システムから出力される各種統計情報は、ISMS などの監査帳票の１つとして利用することも考えている。

また、本システムから教育・啓蒙支援システムに関する機能を切り出すことにより、情報セキュリティマネジメント以外にも、品質管理システムなど組織内の規則や規定などを浸透および遵守させることが重要な分野で同様に利用できる。こちらの製品化について現在準備を進めている。

6. 研究開発の到達目標

現在のシステムでは、啓蒙のための手法として、監視とテストが主体となっているが、インシデント発生を「体験」できるシミュレーション機能を加えたい。これにより、コンテンジェンシー・プランをサポートするツールとしても使用することができるようになる。また、必要に応じて他のシステムと連携し、ダイナミックな実規制が可能となる情報セキュリティ

システムへの発展も計画している。例えば、アクセスコントロールシステムと連携し、情報セキュリティポリシーから逸脱した行動を行った者に対して、自動的にネットワーク上の情報資産に対する物理的なアクセスを規制できるようにする。

本システム単体でも、端末監視対象項目を増やすことや、蓄積された各種統計情報をさまざまな切り口で視覚化し、多面的に分析できるようにすること、自律的に運用管理者にアドバイスを行うことなどを考えている。

また、現在はソフトウェアのみの提供であるが、今後は OS からインストール可能なソフトウェアアプライアンスやサーバとのアプライアンスのような提供形態も考えている。

連絡先
組織名：富士通関西中部ネットテック(株)
部署名：ソリューション統括部
電話：06-6949-3702
URL：http://www.kcn.fujitsu.com/

(7)施設を守る

■セコム社員証ソリューション　IDONE

研究開発団体：セコムトラストネット(株)

1. 研究開発の目的・ねらい

企業における情報の電子化が進み、個人情報（顧客情報）、有価情報、技術研究情報等の重要な情報が盗聴、漏えい、改ざんなどの脅威にさらされている。本開発は、情報セキュリティの確保を通じて、安心・安全な社会システムの構築に寄与することを目的とし、ICカードを活用した確実な個人認証とアクセスコントロールの実現を目指している。

2. 研究開発に至った経緯

２００５年４月に完全施行される個人情報保護法により、個人情報を取り扱う企業での情報漏えい対策の導入が重要な課題となっている中、物理的セキュリティ、情報セキュリティで培ったノウハウが活かせる領域と考え、開発をスタートさせた。

3. 研究開発の内容（特徴）

従来、企業に導入されている社員証を IC カード化し、IC カード内に ID（利用するシステムごとに固有なコード）や電子証明書を格納することにより、一枚の IC カード（社員証）でビル、オフィスなどへの物理的なアクセスコントロール、クライアント PC（サーバ）へのログイン制御、ネットワークへのアクセスコントロール、その他ユーティリティ（勤怠管理、食堂清算、等）の管理が可能となる。

本システムの主な機能は、以下の通り。

ID カード機能

IC カードに顔写真や社員証、職員証を印刷することにより、従来の ID カードとして利用可能となる。

入退室管理機能

ビルやオフィスのドア（電気錠）の開閉を制御し、ドアごと、個人ごと、グループごとに入退室の権限設定が可能となる。

デスクトップセキュリティ機能

クライアント PC（サーバ）へのログイン制御、ファイルの暗号化、デバイスやアプリケーションの利用制限、複数パスワードの管理を実現することにより、PC の不正利用防止、外部記憶媒体での情報持ち出し防止、パスワードの漏えい防止が可能となる。

PKI 機能

秘密鍵、電子証明書を IC カードに格納することにより、IC カードを使った個人認証、電子文書への署名、E-mail の暗号化によるセキュリティ強化が可能となる。万が一クライント PC を紛失しても秘密鍵、電子証明書のコピー不正利用を防止することが可能となる。

その他ユーティリティ機能

■勤怠管理機能

IC カードをカードリーダにかざすだけで、正確な出退勤時間を記録するだけでなく、勤務管理業務におけるコストや稼動負担を大幅に軽減する事が可能。効率的な管理が可能となる。

■キャッシュレス機能

IC カードをカードリーダにかざすだけで、現金を介すことなく社内食堂や売店、自動販売機等での清算が可能となる。また、精算管理等の運用業務を効率的にかつ厳密に行うことが可能とる。

4. 研究開発の課題

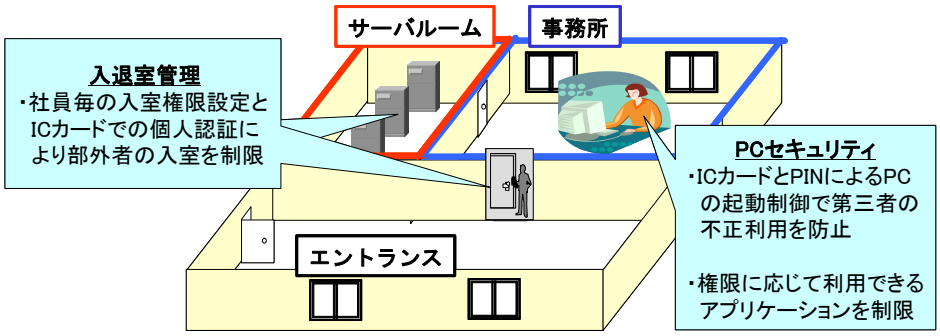
現状、IC カードに格納する ID がアプリケーションやシステムごとに固有であることが多いため、利用するアプリケーションやシステムごとにこれらの ID 管理を行う必要がある。社員の退職や組織変更などにより、複数システムにおける各社員の利用権限の失効処理・変更処理を適時、確実におこなうことは、管理業務の負荷の増大を招くため、いかに効率よく、シンプルに運用・管理できる仕組みを開発するかが課題である。

5. 導入事例・利用イメージ

【導入事例１：オフィス内のセキュリティ強化】

IC カードを利用した入退室管理システムと PC セキュリティの導入を提案

■利用イメージ



■導入効果

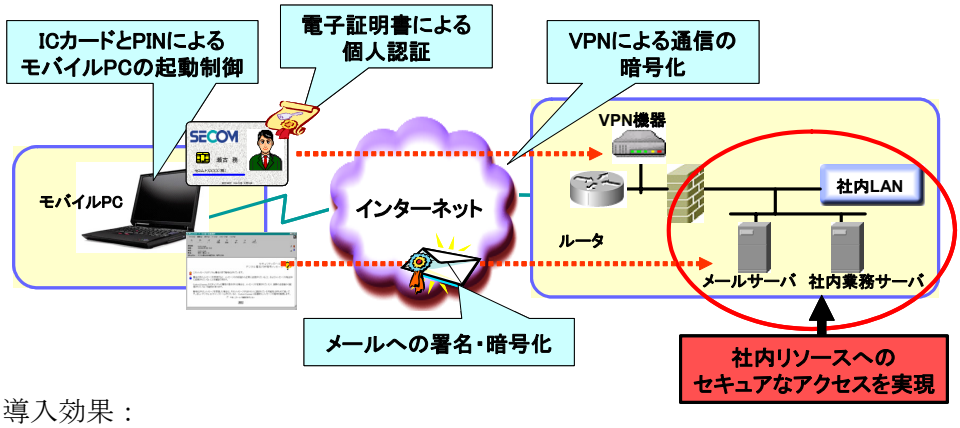
①正社員、契約社員それぞれの権限に応じた部屋への入退室管理を実現。

②『誰が』、『いつ』オフィスに入室したかというログを収集することにより、ユーザの“セキュリティ”への意識付けに成功。

③PC のスクリーンロック機能と入退室管理を組み合わせることで、スクリーンロックの運用ルール徹底を実現。

【導入事例２：モバイル PC のセキュリティ強化】
IC カードを利用したモバイル PC セキュリティと PKI ソリューションの導入

■利用イメージ

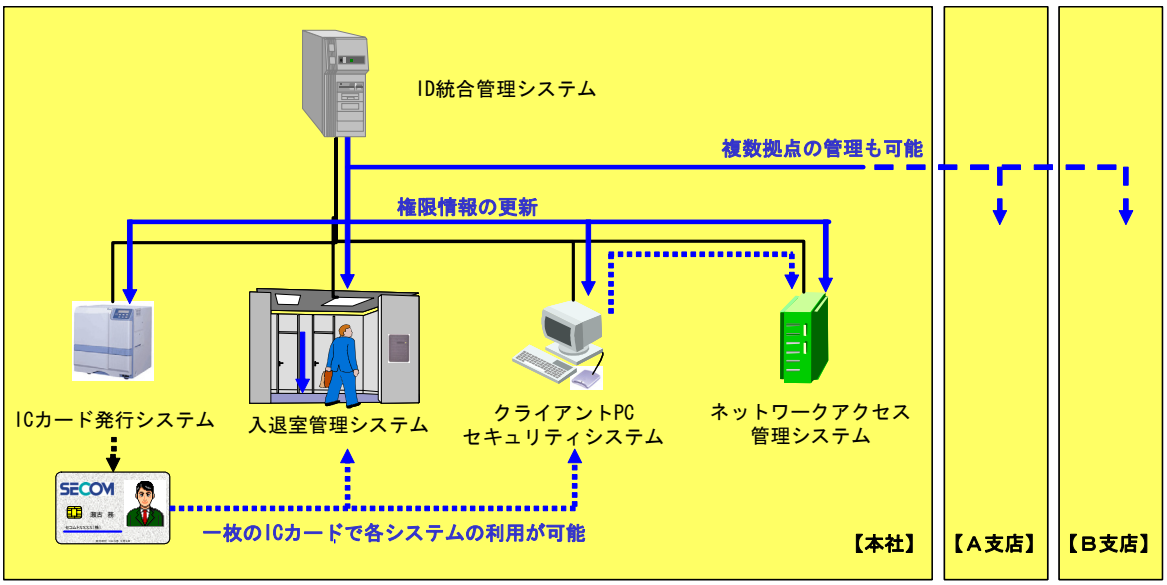


■導入効果：
①IC カードと PIN（ID・パスワード）の組み合わせによる PC の起動制御により モバイル PC の置き忘れ、盗難による情報漏えい防止対策を実現。
②インターネット経由で社員を特定して社内サーバを利用させることを実現

6. 研究開発の到達目標

企業にもとめられる個人情報（顧客情報）、有価情報、技術研究情報等の重要な情報へのセキュリティ強化を図るだけでなく利便性の高いシステムの実現を目標に研究開発を行っている。

短期的な目標としては､企業におけるセキュリティシステムの管理業務の負荷を軽減するために、ID 統合管理システムによる複数システム、複数拠点の統合管理を実現する。



連絡先
組織名：セコムトラストネット株式会社
住所：〒150-0001　東京都渋谷区神宮前１－５－１　セコム本社ビル
電話：０３－５７７５－８７３０
URL：http://www.secomtrust.net/

第３章

調査結果
（データ）

第3章　調査結果（データ）

1. 研究開発の傾向

『解答用紙 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

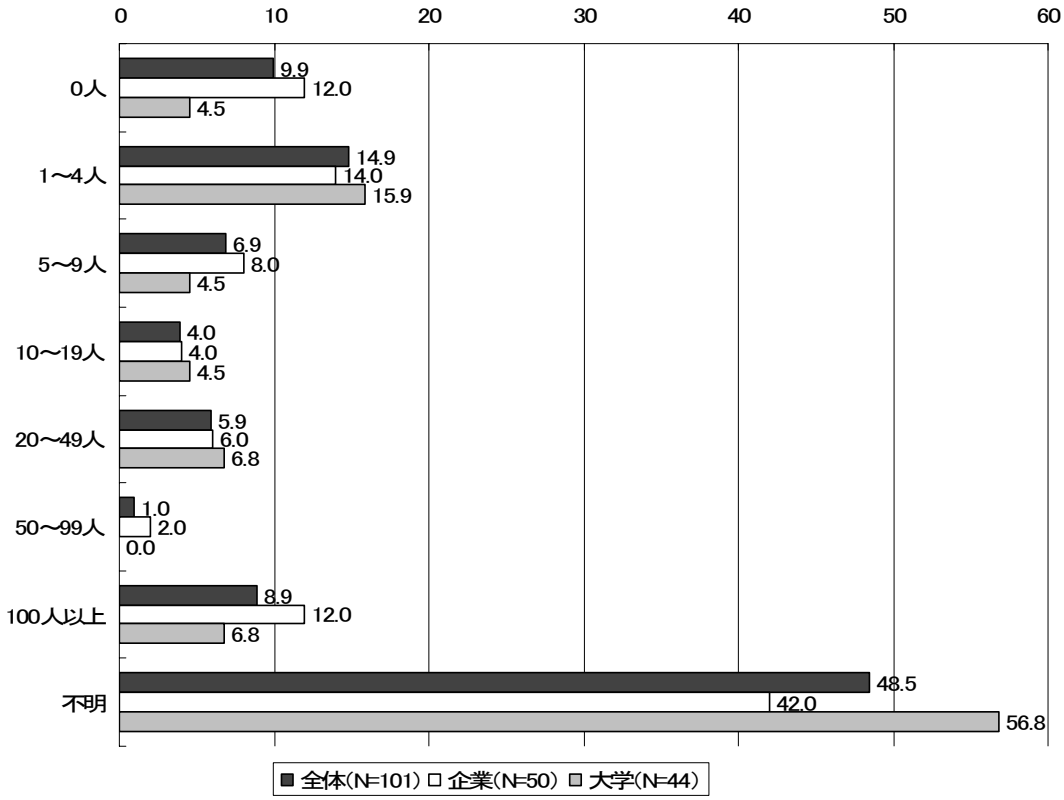
(1) 研究開発に携わっている人数

【本調査】
- ○ 企業・大学全体を見ると、「１～４人」の割合が最も高く、次いで「０人」、「１００人以上」の割合が高い。「少人数で取り組んでいる」、若しくは「相当な人数を掛けている」という「二極化」の傾向が見られる。これは、企業および大学についても同様である。

【経年比較】
- ○ 全体で見ると、「１０～４９人」の割合が急激に減少し、「０人」および「１００人以上」の割合が増加している。研究開発に携わる人員の「少人数化」および「大規模化」の方向に動いている。
- ○ 企業について見ると、上記とほぼ同じ傾向にある。
- ○ 大学について見ると、「１～４人」および「５～９人」の割合が増加し、それ以外では減少している。少人数化（１０人以下のユニット化）の傾向が見られる。

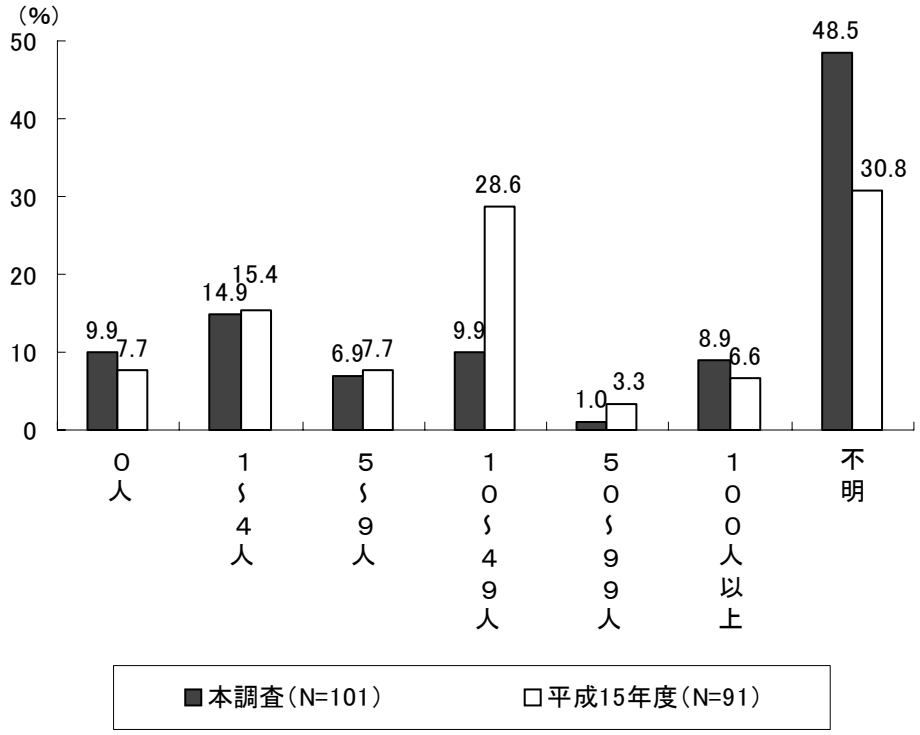
【本調査】

企業・大学全体、企業および大学のいずれにおいても、「１～４人」の割合が最も高く、本調査時点で、これが研究開発の規模として最も手頃な大きさということになる。そして、これに次いで多いのが、「０人」、「１００人以上」である。「少人数で取り組んでいる」、若しくは「相当な人数を掛けている」という「二極化」の傾向が見られる。



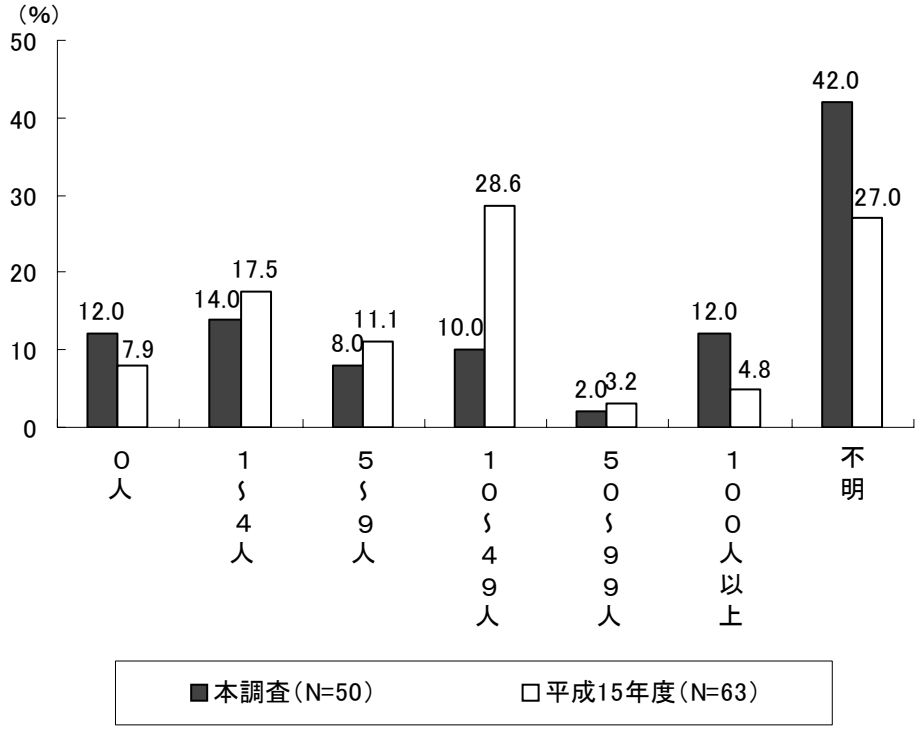
【経年比較（全体)】

平成１５年度調査で最も割合が高かった「１０～４９人」が本調査では急激に減少した。逆に、「０人」および「１００人以上」の割合が増加した。研究開発に携わる人員の「少人数化」あるいは「大規模化」の方向に動いているように見える。ただし、本調査と平成１５年度調査の調査対象が同一でないため、純粋な時系列変化を示唆するものではない。



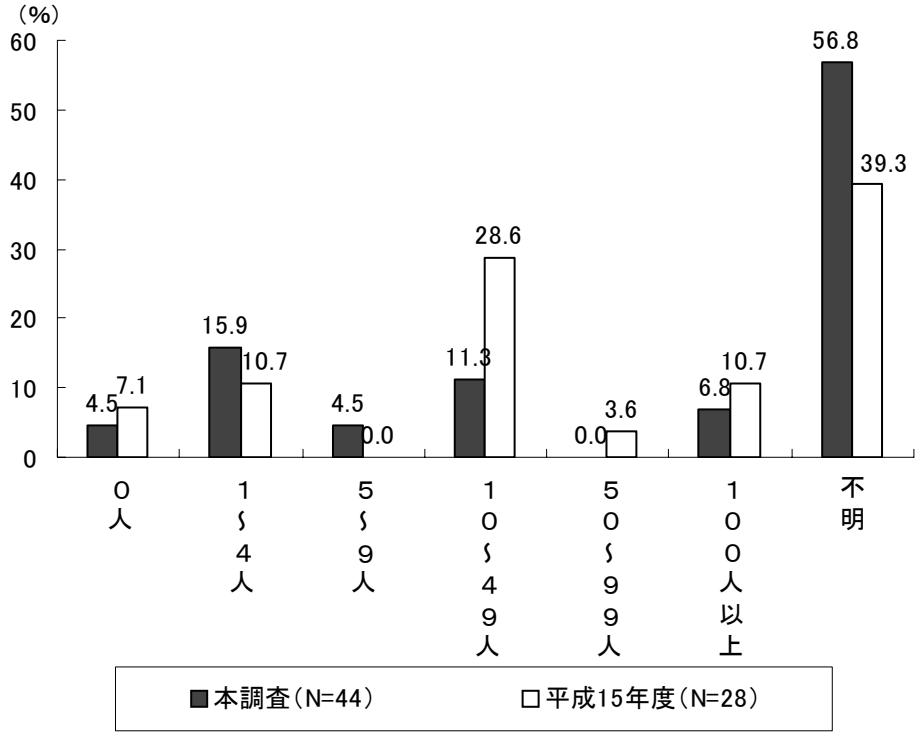
【経年比較（企業)】

企業については、減少傾向が見られる中、「１００人以上」および「０人」の割合が増えていることが大きな特徴と言える。



【経年比較（大学)】

大学については、「１０～４９人」、「５０～９９人」および「１００人以上」の割合が減少し、「１～４人」および「５～９人」の割合が増加している。少人数化（１０人以下のユニット化）の傾向が見られる。



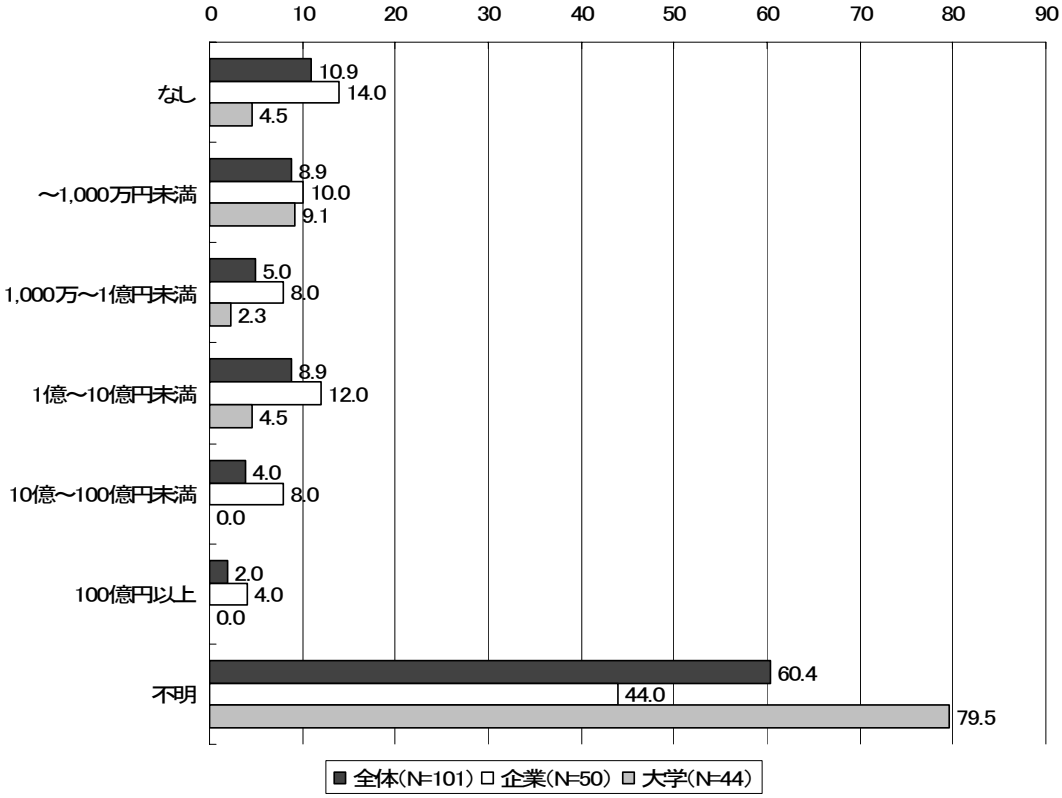
(2)年間の研究開発費

【本調査】
- ○ 企業・大学全体を見ると、「１，０００万円未満」および「１億～１０億円」の割合が比較的高い。研究開発費から見た、本調査時点での研究開発の規模感としては、数百万円規模の研究開発と数億円規模の研究開発があるように見える。

【経年比較】
- ○ 全体で見ると、「１，０００万～１億円」および「１億円以上」の割合が減少し、「なし」および「１，０００万円未満」の割合が増加している。研究開発費の削減傾向が見られる。
- ○ 企業における研究開発費が、１，０００万円および１億円を境にして、より小額化および高額化の傾向が見られる。
- ○ 大学について見ると、「１，０００万円未満」の割合が増加していることから、数百万円程度の研究開発費で行える規模のものが中心である。

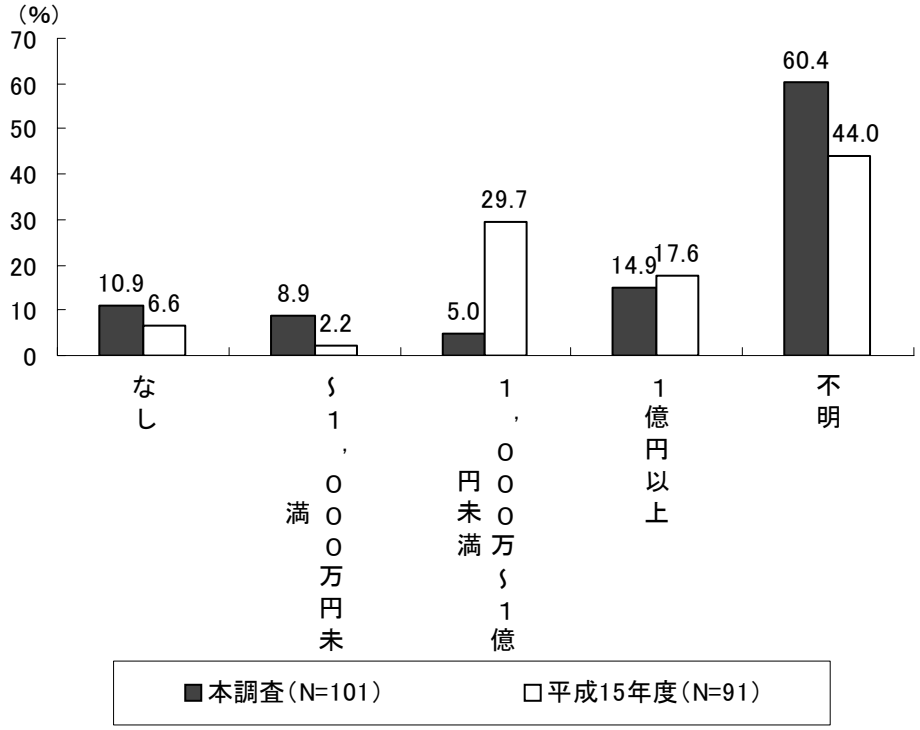
【本調査】

企業・大学全体、企業および大学のいずれにおいても、「１，０００万円未満」および「１億～１０億円」の割合が比較的高い。研究開発費から見た、本調査時点での研究開発の規模感としては、数百万円規模の研究開発と数億円規模の研究開発があるように見える。



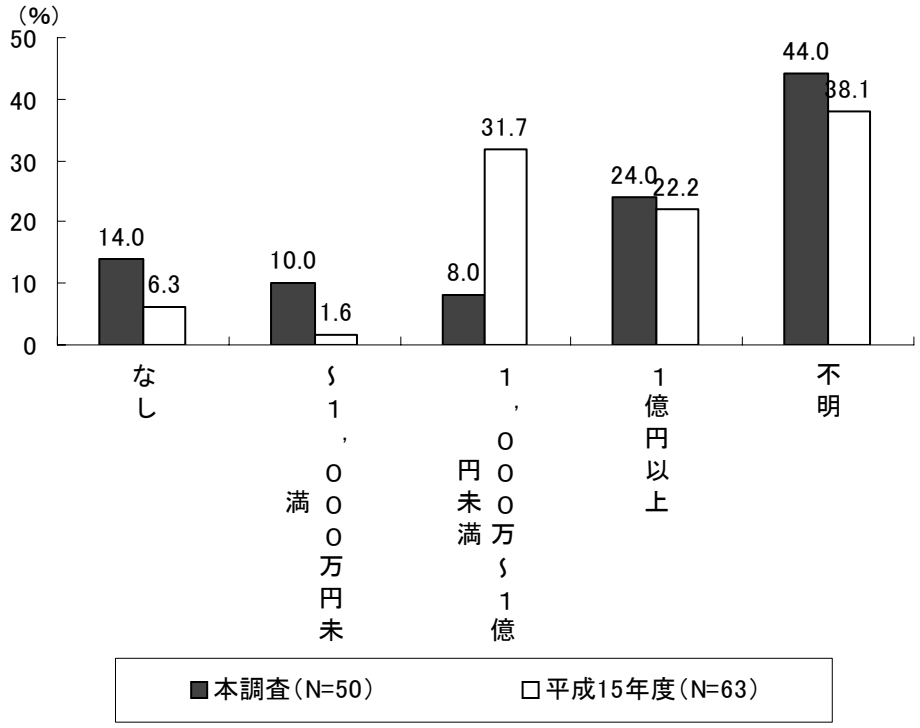
【経年比較（全体)】

全体で見ると、「１，０００万～１億円」および「１億円以上」の割合が減少し、「なし」および「１，０００万円未満」の割合が増加している。研究開発費の削減傾向が見られる



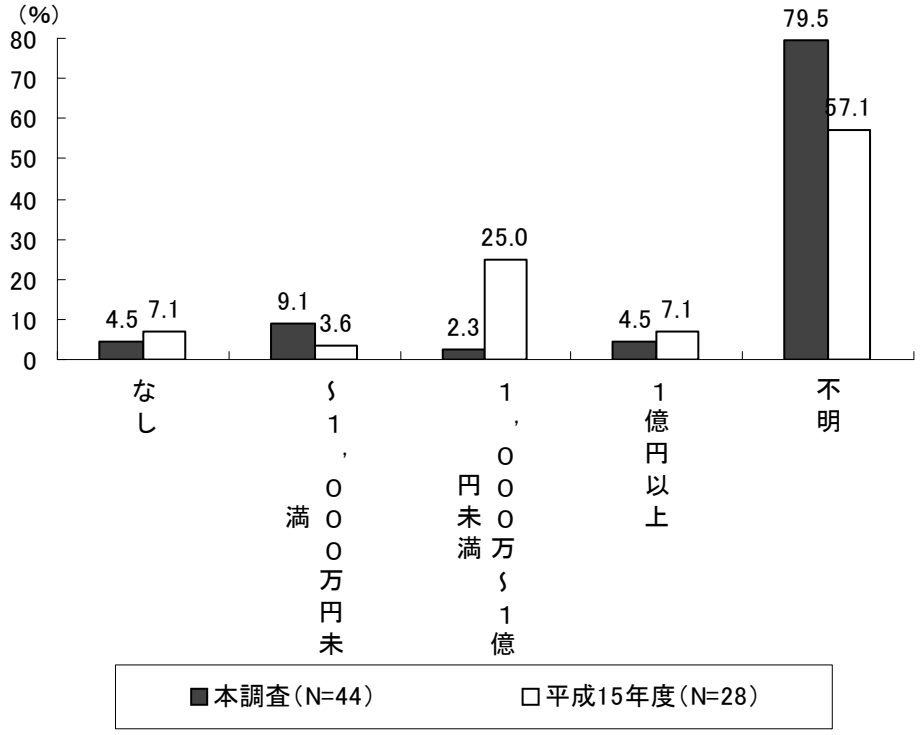
【経年比較（企業)】

企業について見ると、「１，０００万～１億円」の割合が減少し、「なし」および「１，０００万円未満」が増加している。また、「１億円以上」も微増ながら増加している。企業における研究開発は、１，０００万円および１億円を境にして、おおよそ数百万円程度で行える規模のものと数億円規模のものが主流になりつつある。



【経年比較（大学)】

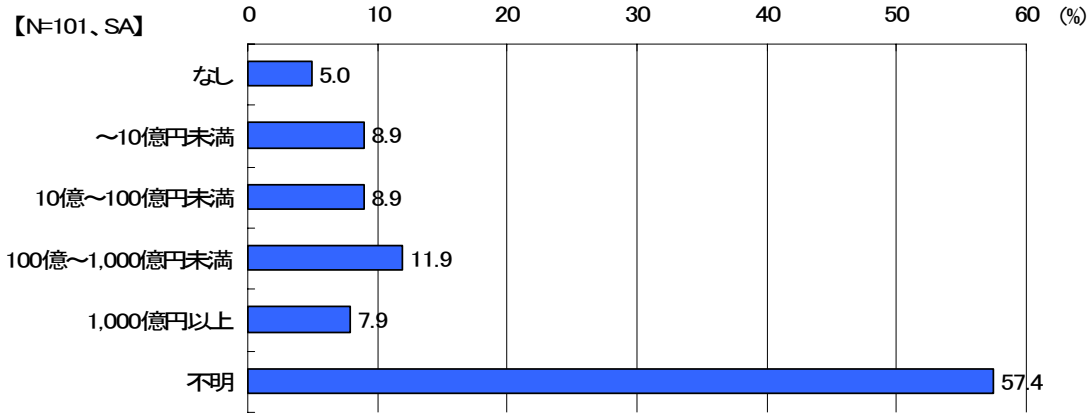
大学について見ると、「１，０００万円未満」の割合が増加し、それ以外は減少している。大学における研究開発は数億円規模のものもあるが、おおよそ数百万円程度で行える規模のものが中心のようである。



(3)年間売り上げ（全体）

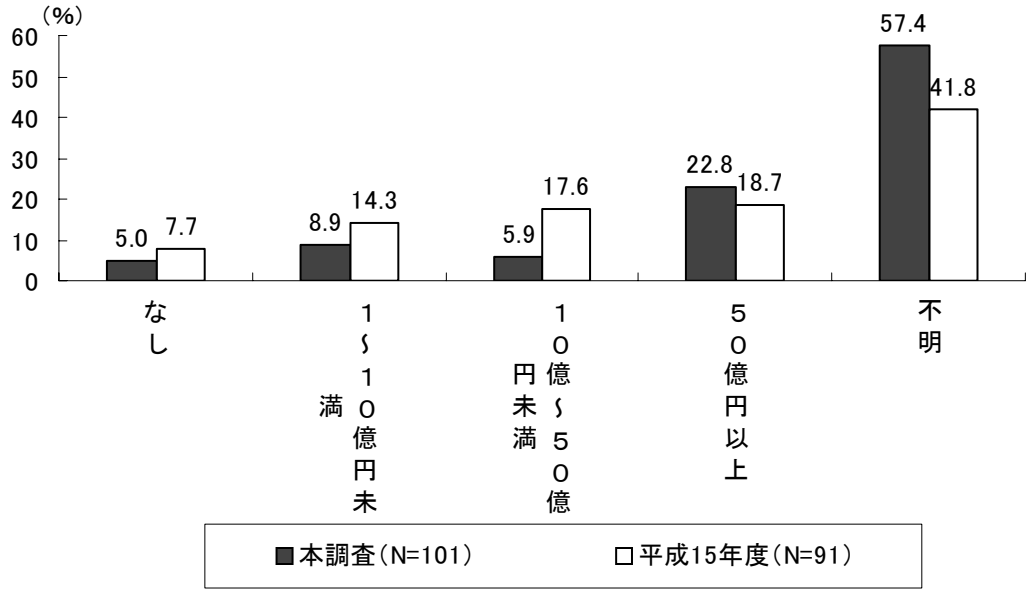
【本調査】

本調査対象の企業の年間売り上げを見ると、数百億円規模の企業が多い。



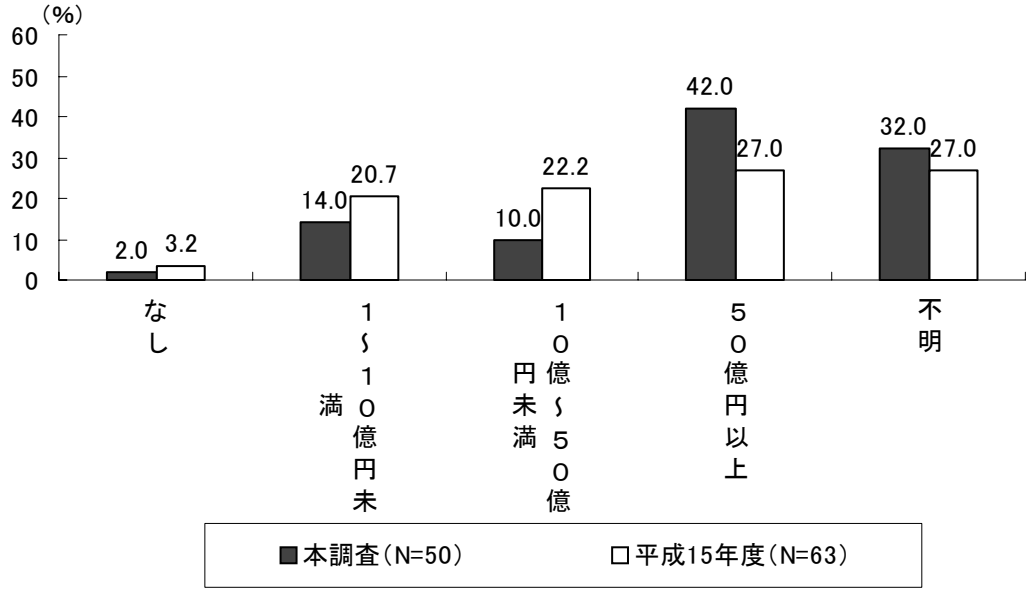
【経年比較（全体)】

平成１５年度調査と比較すると、全体としては年間売り上げ規模が拡大している。



【経年比較（企業)】

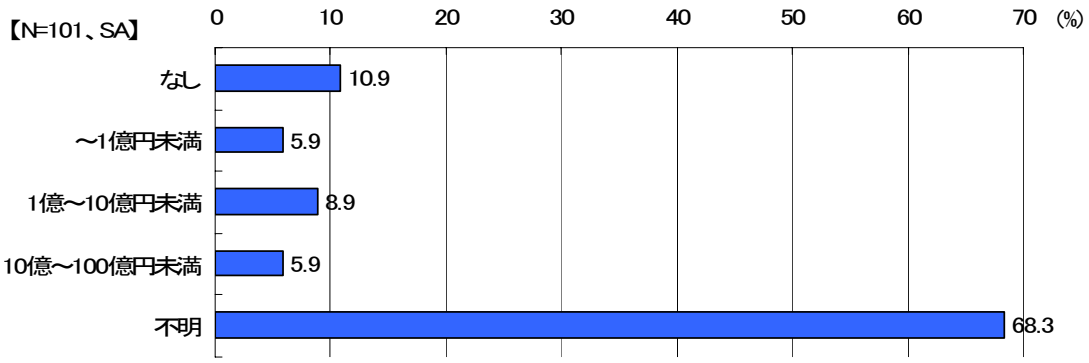
平成１５年度調査と比較すると、本調査における企業は年間売り上げ規模が拡大している。



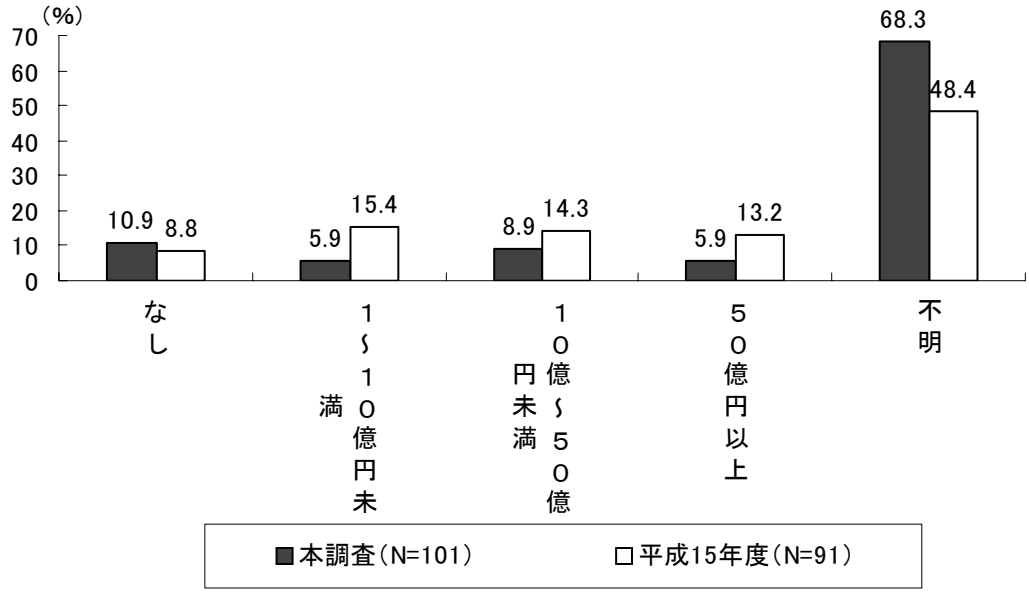
(4)年間売り上げ（アクセス制御関連）

【本調査】

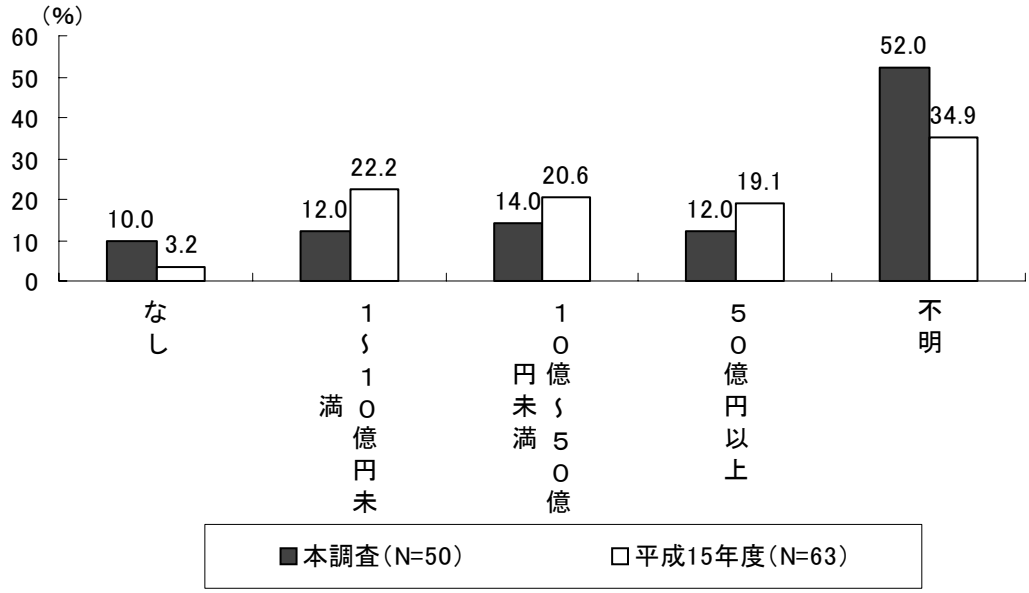
企業におけるアクセス制御関連の年間売り上げは、各層、平均的に存在する。一方、大学についてはアクセス制御関連の年間売り上げはない。



【経年比較（全体）】
平成１５年度調査と比較すると、アクセス制御関連の年間売り上げは減少している。



【経年比較（企業）】
平成１５年度調査と比較すると、企業におけるアクセス制御関連の年間売り上げが減少している。



1.2 現在、取り組んでいる分野

【本調査】

○ アクセス制御機能に関する技術の研究開発に現在、取り組んでいる企業・大学は、６５であり、これは本調査回答数の６９．１％に相当する。これを平成１５年度調査と比較すると、７．８ポイントの減少となっている。

○ 現在、企業・大学が取り組んでいる研究開発分野を見ると、全体としては「ネットワークセキュリティ（４３．６％）」および「認証技術（４０．６％）」の割合が比較的高い。

○ 平成１５年度調査では、「今後、最も力を入れていく分野」として、「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」、「セキュリティサービス関連」が上位に挙げられているが、本調査はこれを反映したものとなっている。

○ 企業について見ると、比較的取り組み割合が高い分野と低い分野に分けることができ、緩やかな「二極化」の傾向が見られる。

［比較的取り組み割合が高い分野］	［比較的取り組み割合が低い分野］
認証技術	暗号技術
セキュリティサービス関連	ウイルス対策
ネットワークセキュリティ	
セキュリティマネジメント	
不正侵入対策	

○ 大学について見ると、全ての分野について平均的に取り組まれている。

○「セキュリティサービス関連」については、企業と大学で取り組み割合が多い。一方、「暗号技術」については、大学での取り組み割合が高い。

【経年比較】

○ 全体で見ると、取り組み分野ごとに、上昇傾向・下降傾向・現状維持の３つの傾向が見られる。

［上昇傾向］	［下降傾向］	［現状維持］
ウイルス対策	暗号技術	セキュリティマネジメント
不正侵入対策	認証技術	セキュリティサービス関連
	ネットワークセキュリティ	

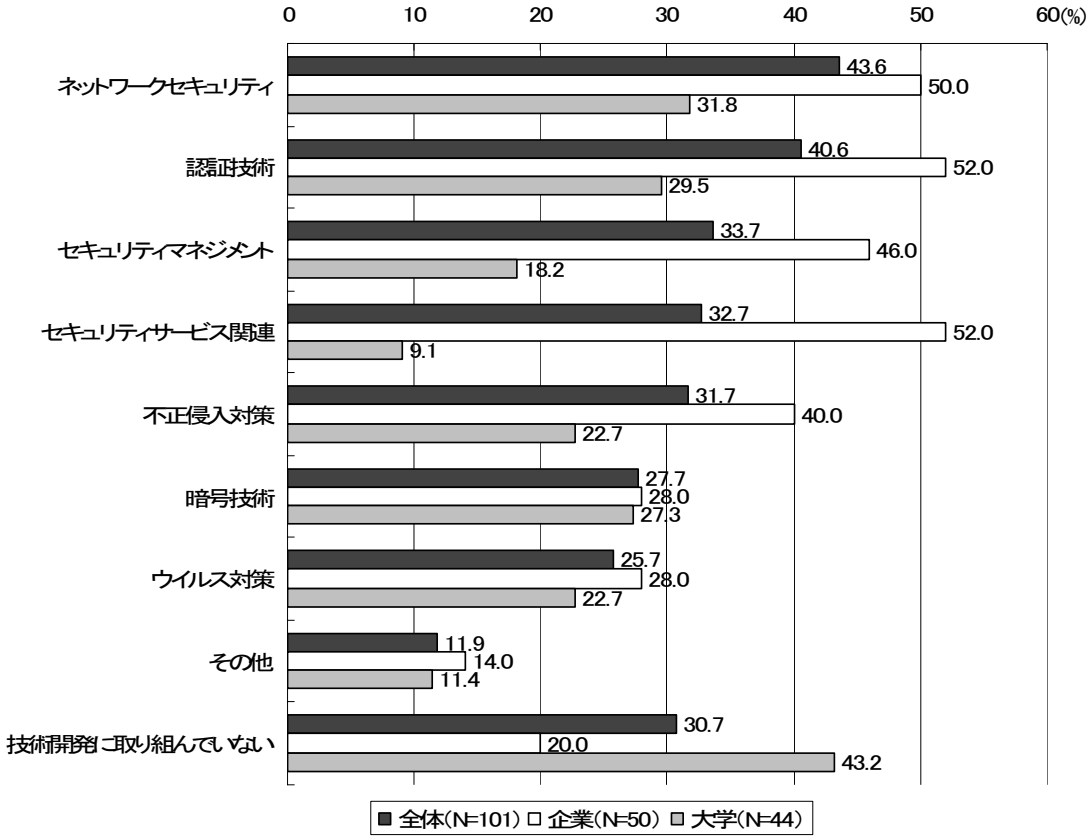
○ 企業では、「不正侵入対策」、「ウイルス対策」および「セキュリティサービス関連」の取り組み割合が高くなっている。一方、大学では、「ウイルス対策」の取り組み割合が高くなっている。

【本調査】

企業・大学が取り組んでいる研究開発分野を見ると、全体としては「ネットワークセキュリティ（４３．６%）」および「認証技術（４０．６%）」の割合が比較的高い。また、「セキュリティサービス関連」については企業と大学で取り組みに大きな差異が出ている。一方、「暗号技術」については、大学では取り組み割合が高い。

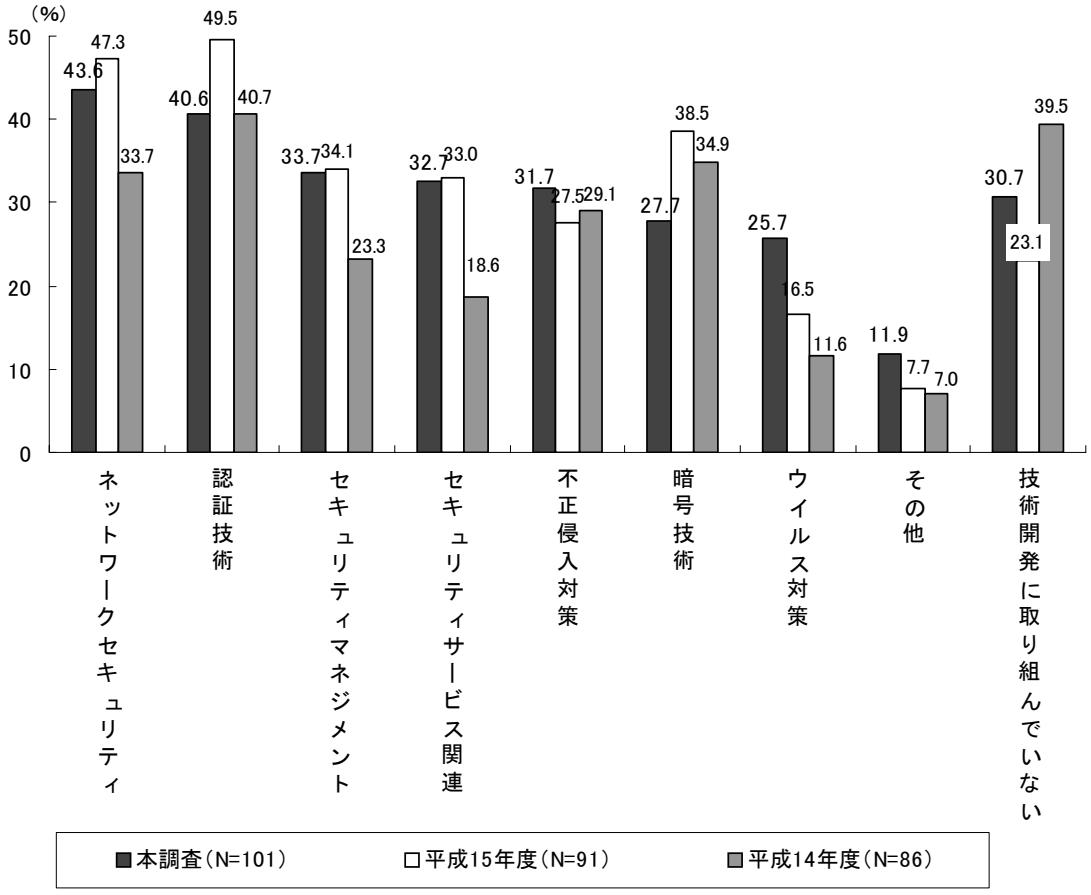
企業の特徴としては、比較的取り組み割合が高い分野と低い分野に分けることができ、緩やかな「二極化」の傾向が見られる。

大学の特徴としては、全ての分野について平均的に取り組まれている。



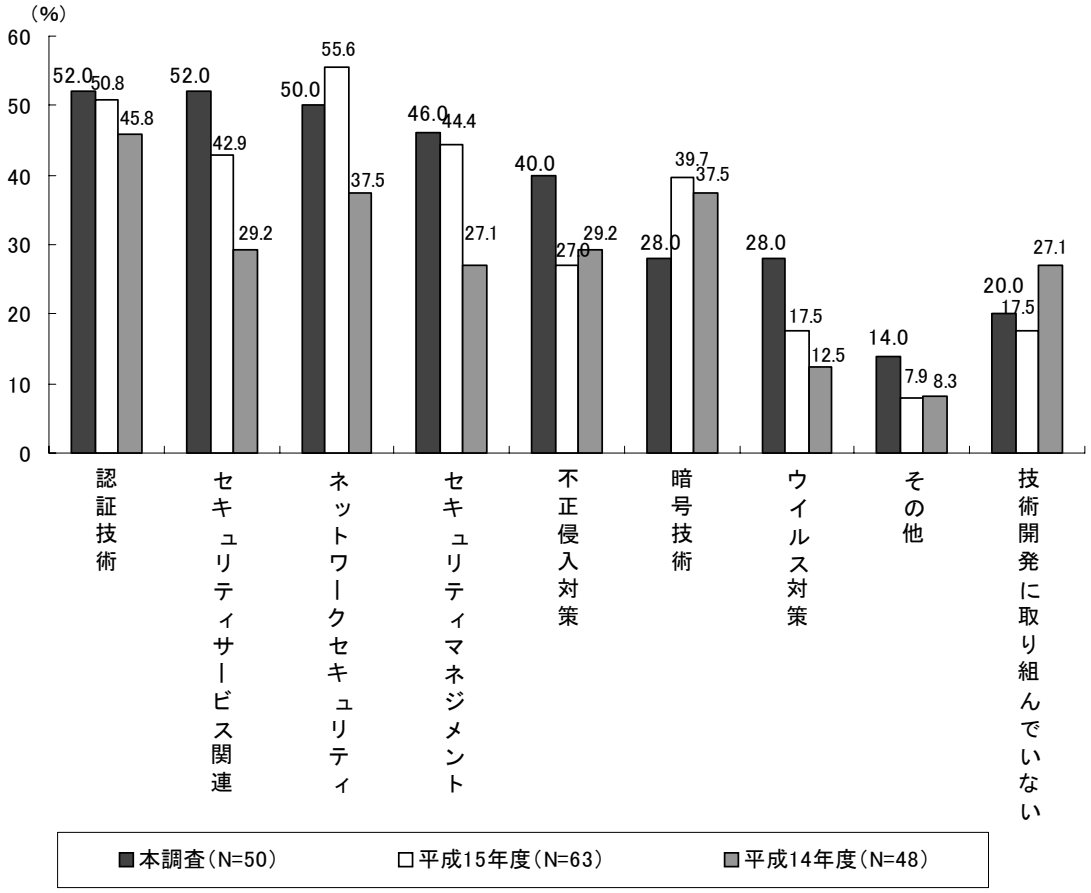
【経年比較（全体）】

平成１５年度調査と比較すると、ウイルス対策および不正侵入対策が、上昇傾向にある。



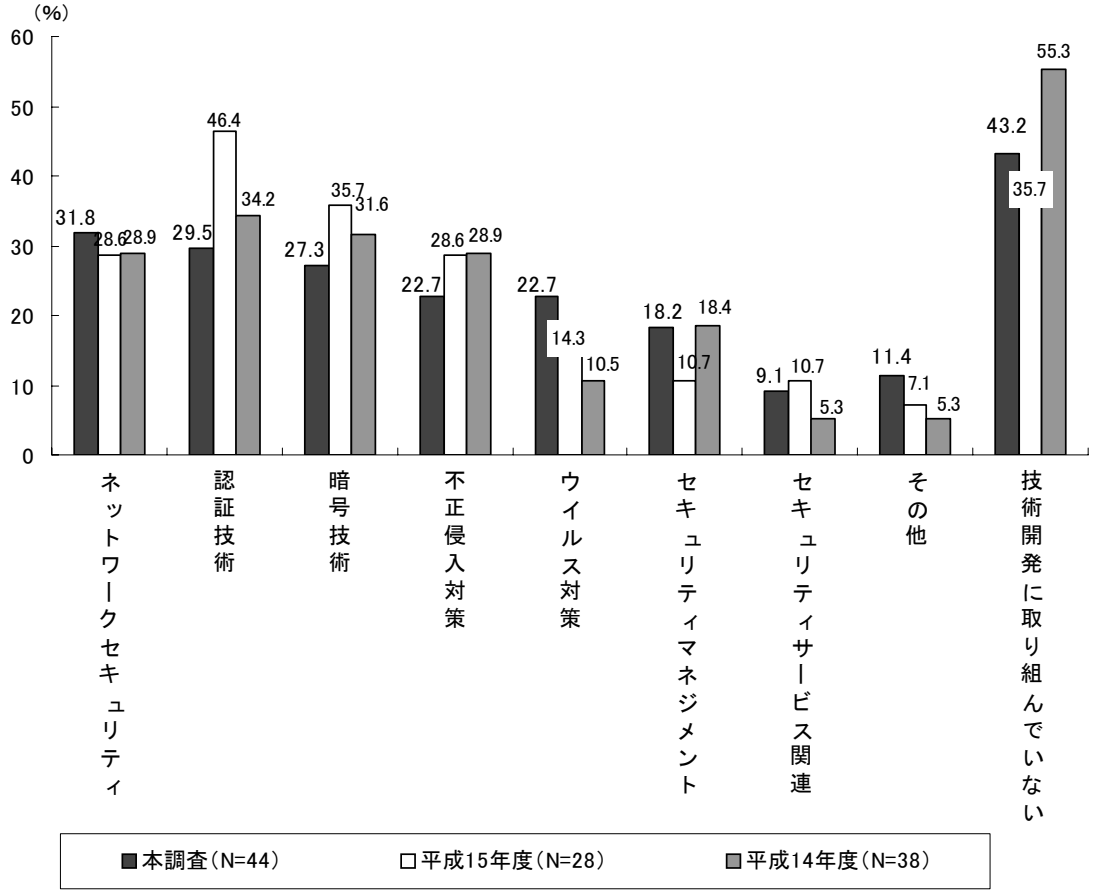
【経年比較（企業)】

平成１５年度調査と比較すると、「不正侵入対策」、「ウイルス対策」および「セキュリティサービス関連」の取り組み割合が高くなっている。



【経年比較（大学)】

平成１５年度調査と比較すると、「ウイルス対策」の取り組み割合が高くなっている。



1.3 今後、取り組んでいく分野

【本調査】

○ 企業・大学が今後、取り組んでいく研究開発分野を見ると、全体としては「ネットワークセキュリティ（３３．７%）」が最も高く、次いで「セキュリティマネジメント（３０．７%）」、「認証技術（２８．７%）」、「セキュリティサービス関連（２６．７%）」、「暗号技術（２２．８%）」の順となっている。

○ 企業について見ると、比較的割合が高い分野と低い分野の２つのグループに分けることができる。

［比較的割合が高い分野］	［比較的割合が低い分野］
セキュリティマネジメント	不正侵入対策
認証技術	暗号技術
セキュリティサービス関連	ウイルス対策

○ 大学について見ると、「ネットワークセキュリティ」の割合が比較的高い。

○「セキュリティサービス関連」は、企業と大学では取り組みの姿勢にそれぞれ顕著な差異が見られる。

【経年比較】

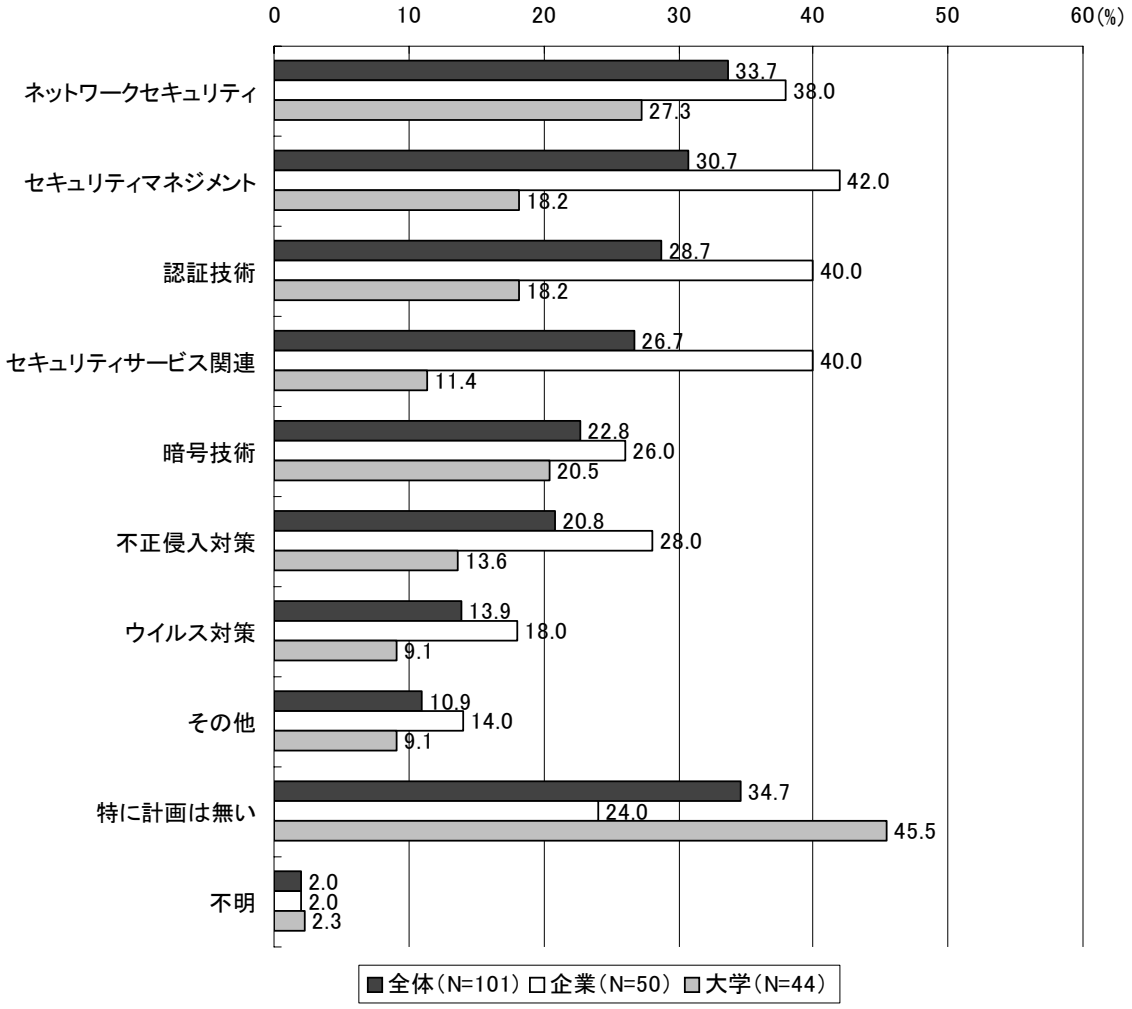
○ 全体、企業および大学のいずれにおいても、ほぼ全ての分野が、総じて、減少傾向にある。ただし、本調査と平成１５年度調査の調査対象が同一でないため、純粋な時系列変化を示唆するものではない。

【本調査】

企業・大学が今後、取り組んでいく研究開発分野を見ると、全体としては「ネットワークセキュリティ（３３．７%）」が最も高く、次いで「セキュリティマネジメント（３０．７%）」、「認証技術（２８．７%）」、「セキュリティサービス関連（２６．７%）」、「暗号技術（２２．８%）」の順となっている。また、「セキュリティサービス関連」について、企業と大学では取り組みの姿勢にそれぞれ顕著な差異が見られる。

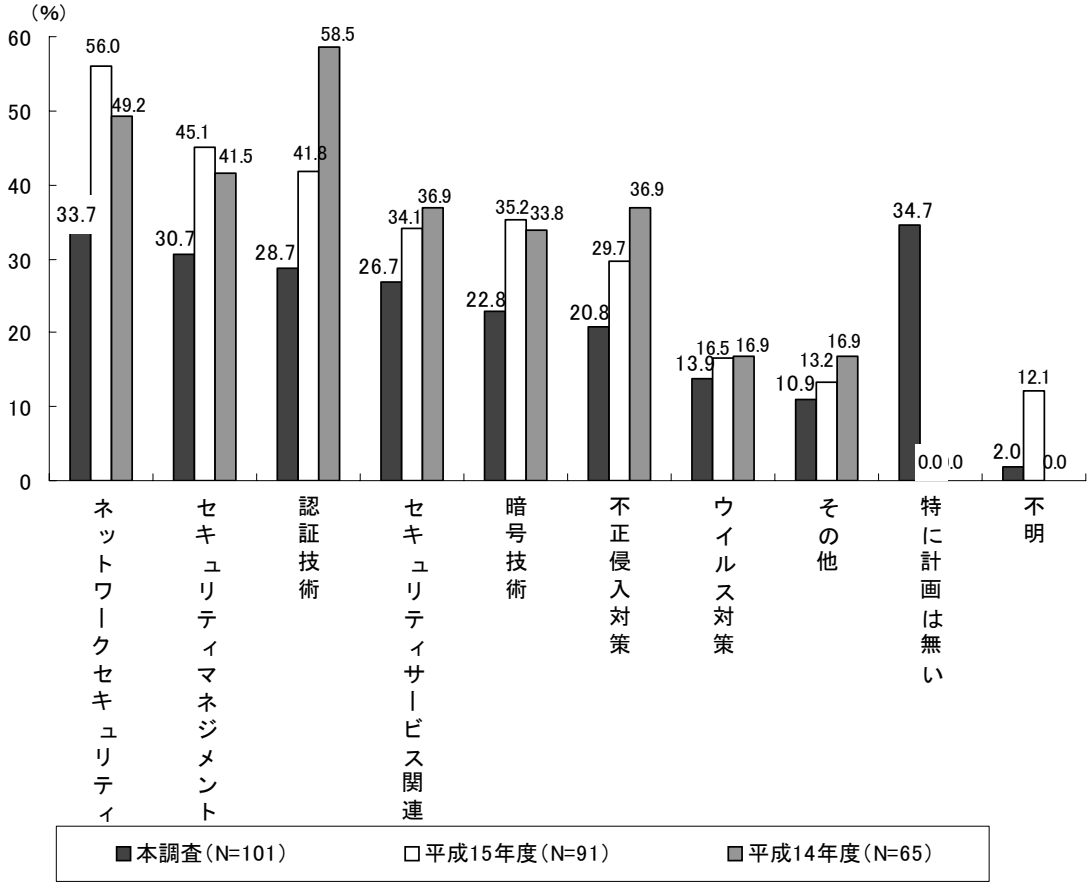
企業の特徴としては、比較的割合が高い分野と低い分野の２つのグループに分けることができる。

大学の特徴としては、「ネットワークセキュリティ」の割合が比較的高い。



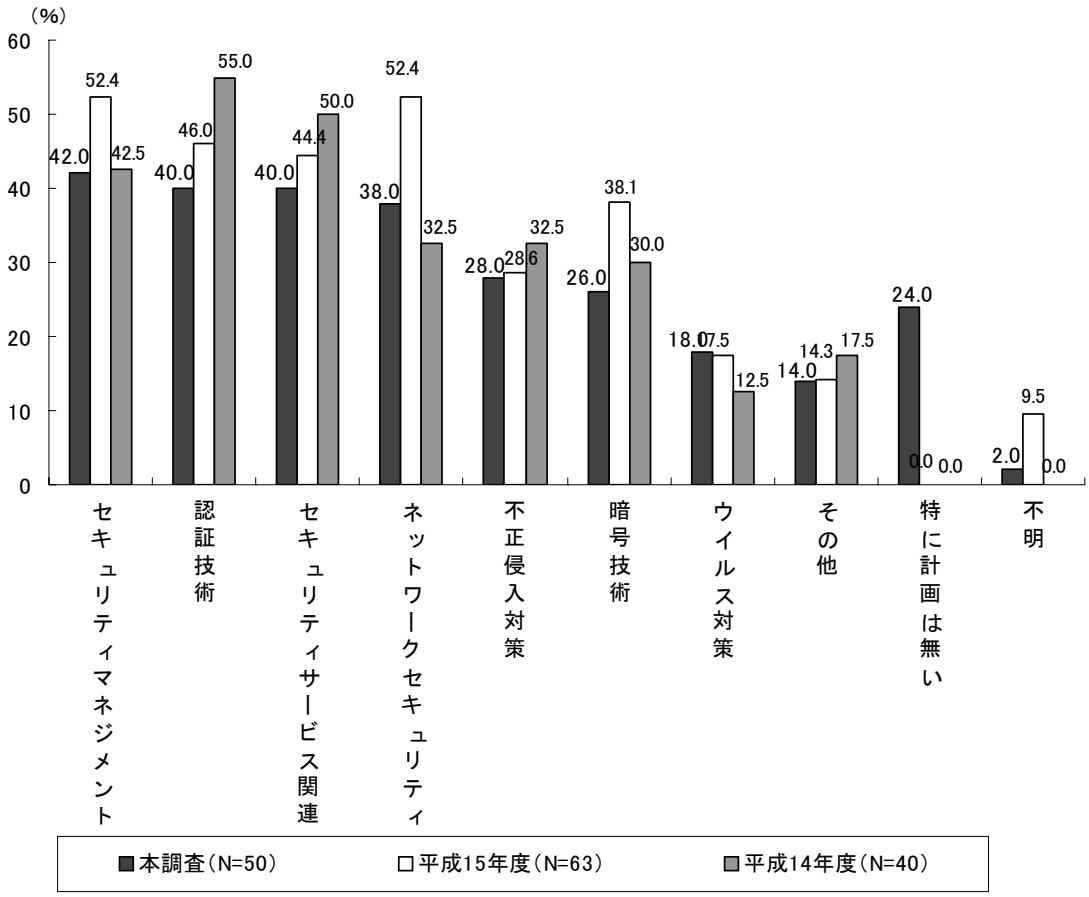
【経年比較（全体）】

平成１５年度調査と比較すると、全ての分野で減少している。



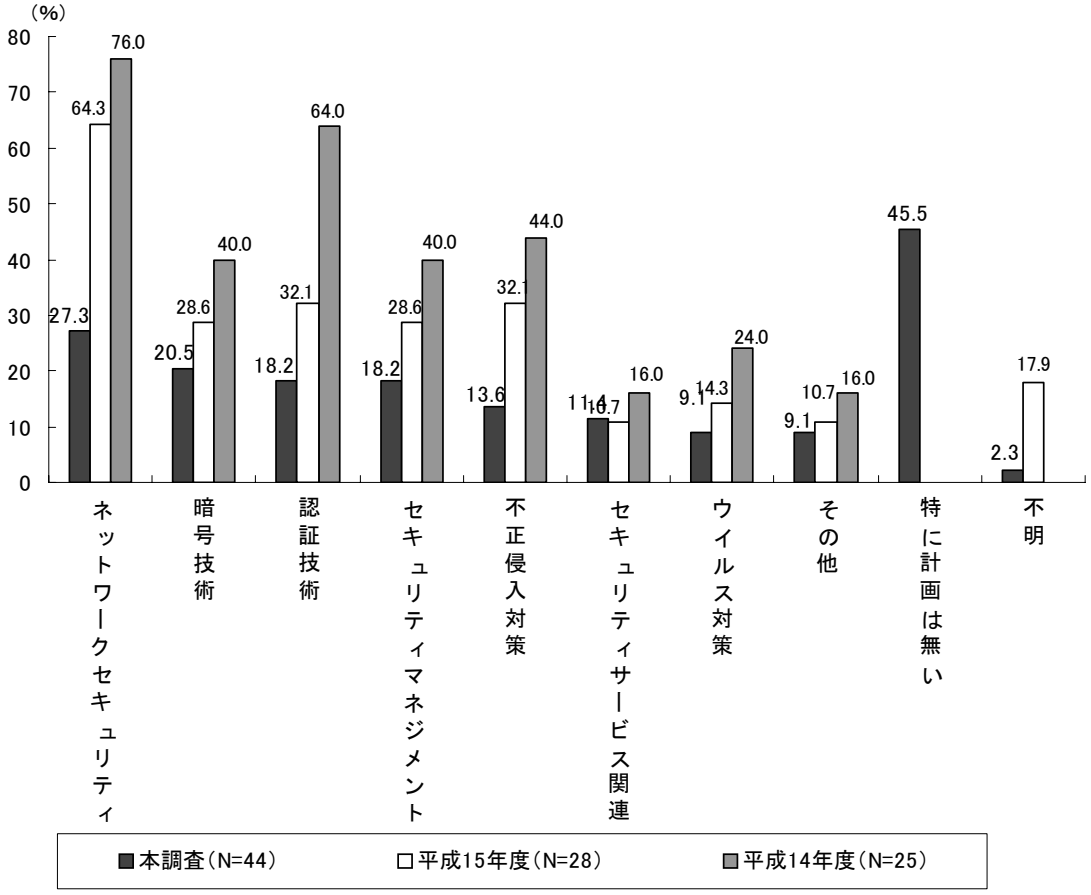
【経年比較（企業)】

平成１５年度調査と比較すると、ほぼ全ての分野で減少しているが、ウイルス対策が若干増加している。



【経年比較（大学)】

平成１５年度調査と比較すると、ほぼ全ての分野で減少している。



1.4 今後、最も力を入れていく分野

【本調査】
- ○ 企業・大学が今後、取り組む予定がある研究開発分野の中で、最も力を入れていく分野は、全体としては「セキュリティマネジメント（１１．９％）」が高い。
- ○ 企業について見ると、比較的割合が高い分野と低い分野の２つの集団に分けることができ、この差が顕著であることから、取り組み分野における「選択と集中」が示唆される。

［比較的割合が高い分野］	［比較的割合が低い分野］
認証技術	暗号技術
セキュリティサービス関連	不正侵入対策
セキュリティマネジメント	ウイルス対策

- ○ 大学について見ると、「セキュリティマネジメント」、「暗号技術」の割合が比較的高い。
- ○「暗号技術」および「セキュリティサービス関連」について、企業と大学では取り組みの姿勢にそれぞれ顕著な差異が見られる。
- ○ 企業・大学に共通するのは、いずれも「不正侵入対策」および「ウイルス対策」が極めて低い。

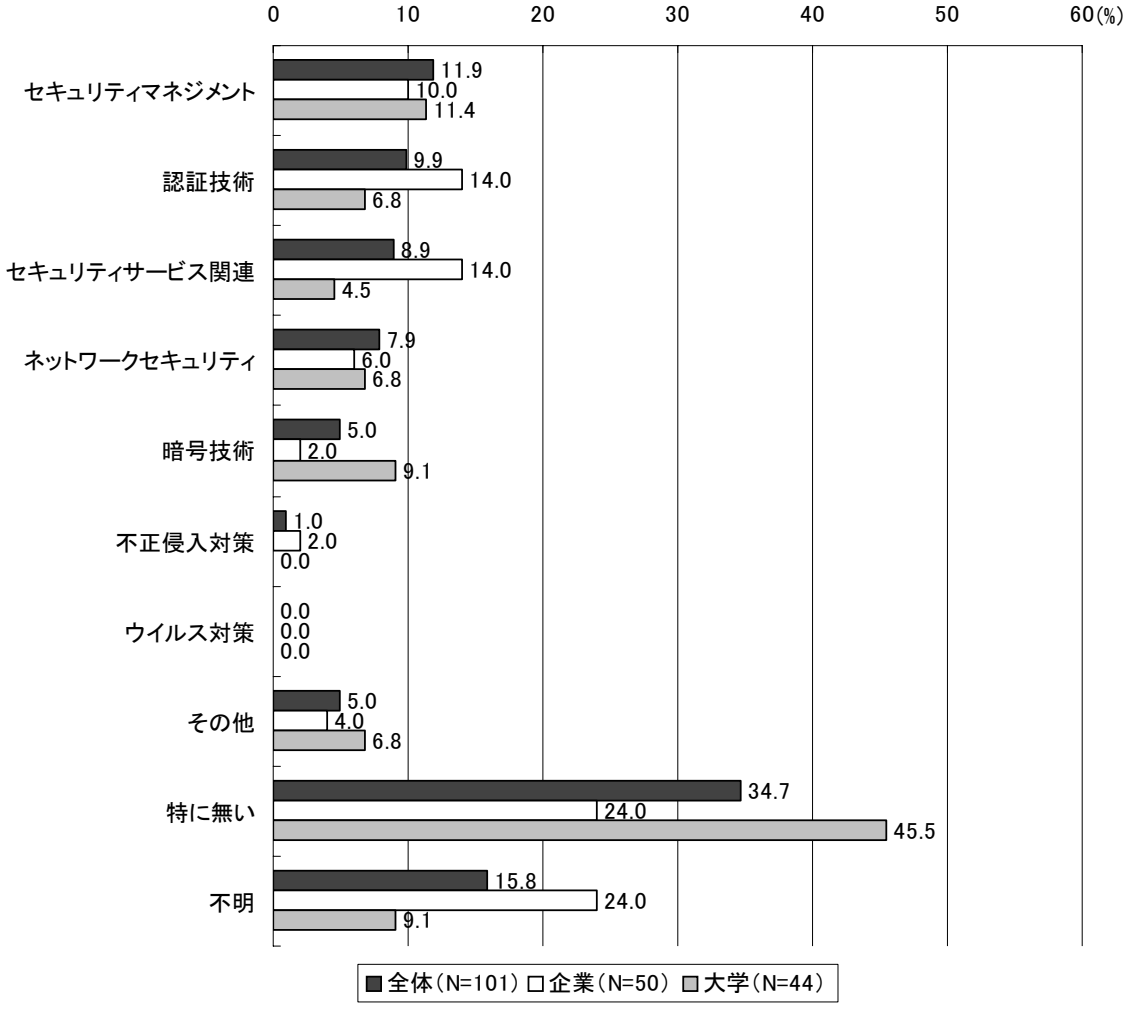
【経年比較】
- ○ 全体で見ると、「暗号技術」および「セキュリティサービス関連」の取り組み割合が増加傾向にある。とくに、前者は大学が、後者は企業が牽引役を担っている。

【本調査】

今後、取り組む予定がある研究開発分野の中で、最も力を入れていく分野は、全体としては「セキュリティマネジメント（１１．９％）」である。また、「暗号技術」および「セキュリティサービス関連」について、企業と大学では取り組みの姿勢にそれぞれ顕著な差異が見られる。企業・大学に共通するのは、いずれも「不正侵入対策」および「ウイルス対策」が極めて低いことである。

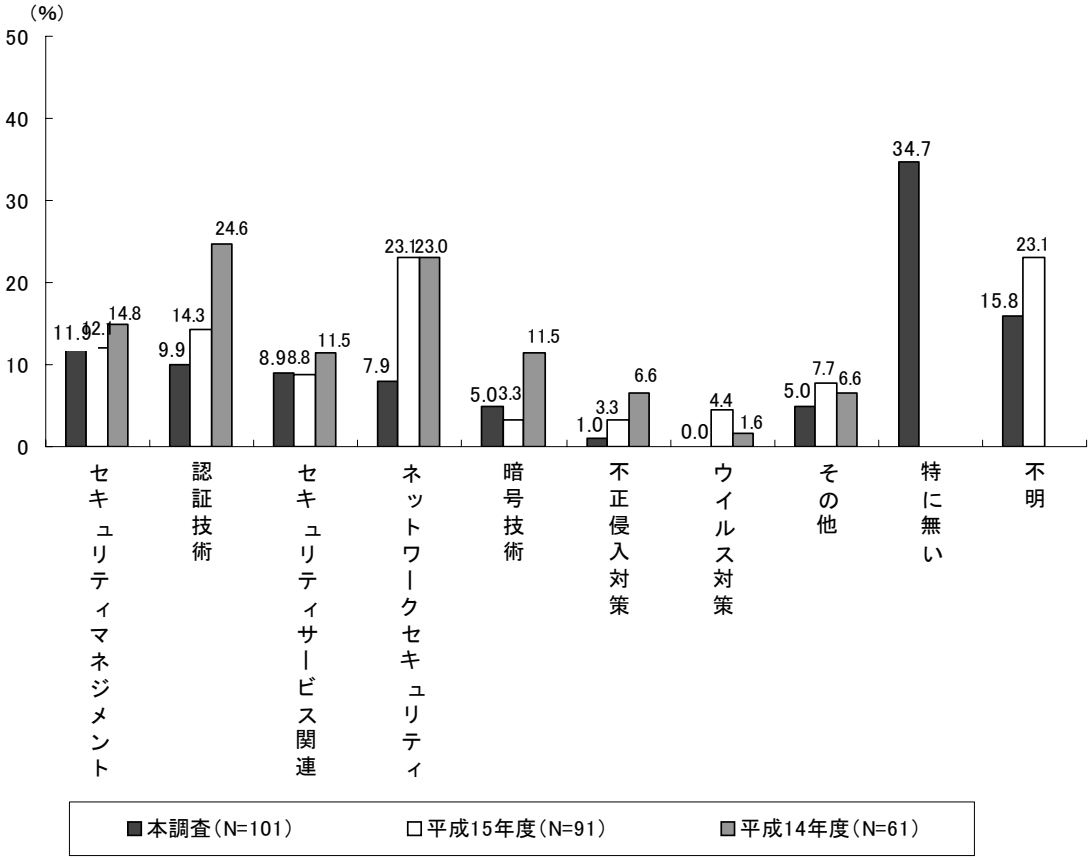
企業の特徴として、比較的割合が高い分野と低い分野の２つのグループに分けることができる。また、両者の差が顕著であることから、取り組み分野における「選択と集中」が示唆される。

大学の特徴として、「セキュリティマネジメント」、「暗号技術」の割合が比較的高い。



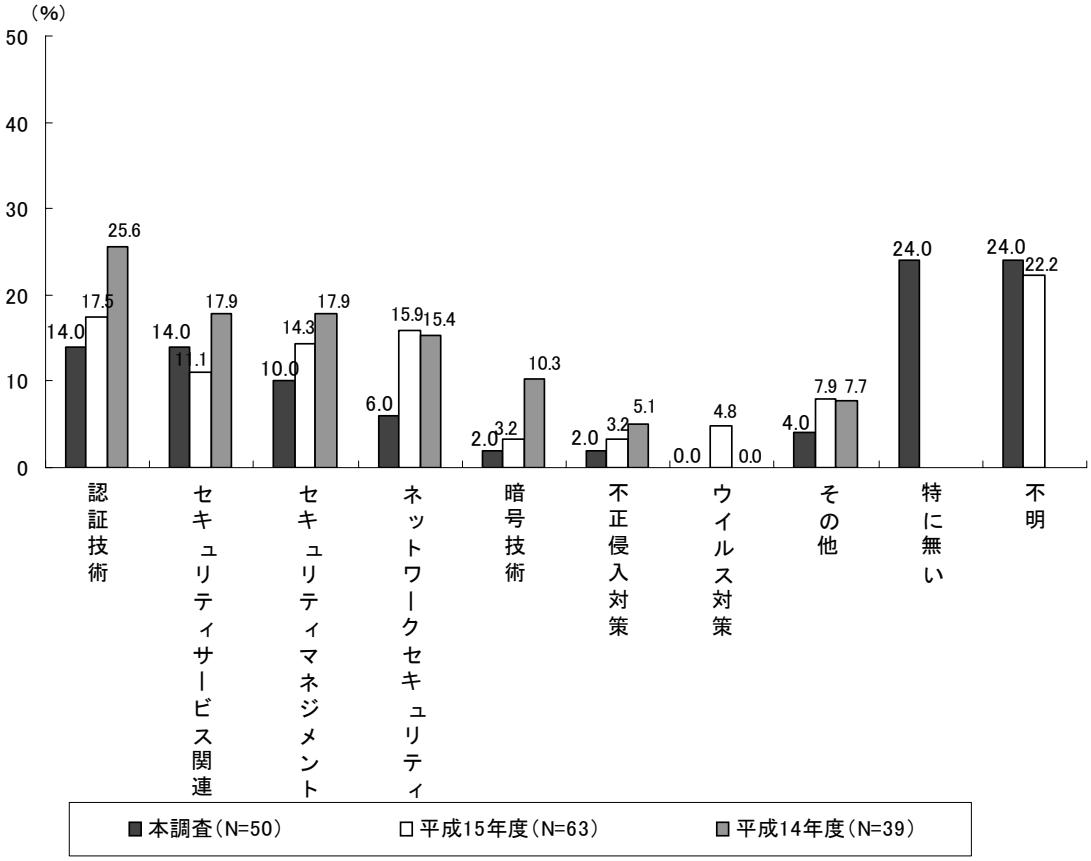
【経年比較（全体）】

平成１５年度調査と比較すると、微増ながら、「暗号技術」および「セキュリティサービス関連」の取り組み割合が増加傾向にあり、これら２分野に対する注目度は高いと言える。ただし、本調査と平成１５年度調査の調査対象が同一でないため、純粋な時系列変化を示唆するものではない。



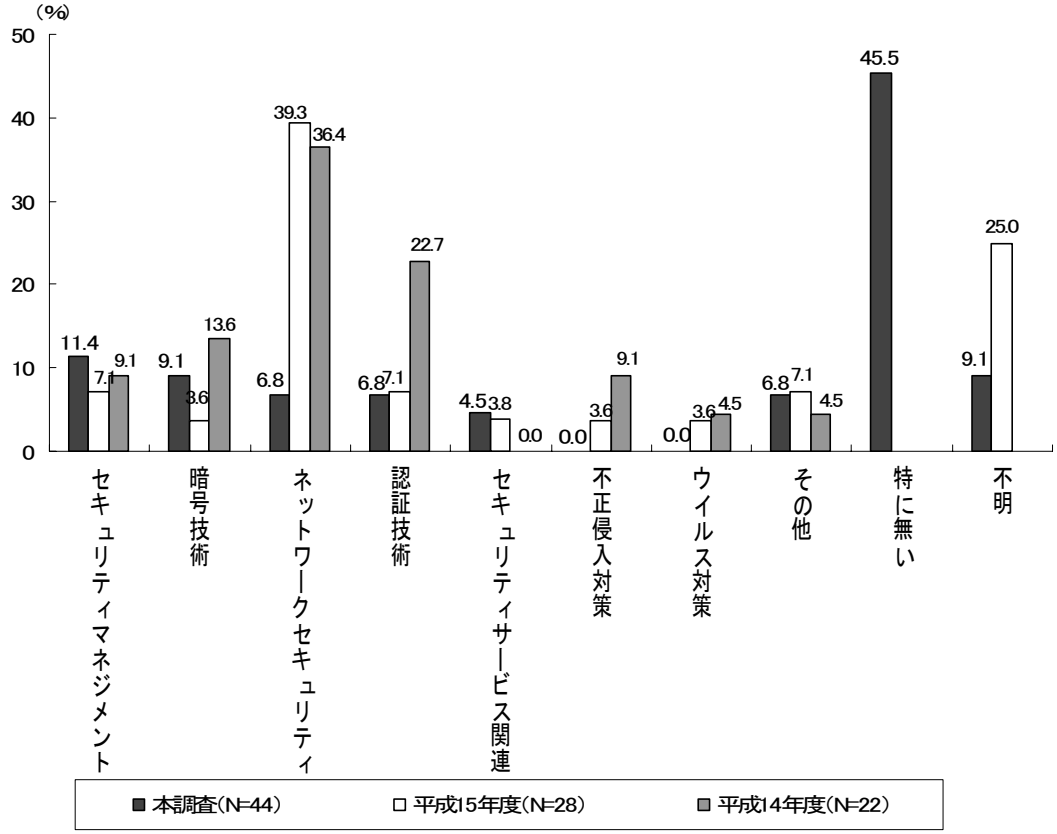
【経年比較（企業)】

平成１５年度調査と比較すると、「セキュリティサービス関連」の取り組み割合が増加傾向にあり、この分野に対する企業の注目度は高いと言える。ただし、本調査と平成１５年度調査の調査対象が同一でないため、純粋な時系列変化を示唆するものではない。



【経年比較（大学)】

平成１５年度調査と比較すると、「セキュリティマネジメント」、「暗号技術」および「セキュリティサービス関連」の取り組み割合が増加傾向にあり、これら３分野に対する大学の注目度は高いと言える。ただし、本調査と平成１５年度調査の調査対象が同一でないため、純粋な時系列変化を示唆するものではない。



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】

- 現在、実用化（製品化）されているアクセス制御機能を見ると、全体としては「ネットワークセキュリティ（２１．８%）」、「認証技術（２０．８%）」、「セキュリティサービス関連（２０．８%）」および「セキュリティマネジメント（１８．８%）」の割合が比較的高い。
- 平成１５年度調査では、「今後、実用化（製品化）を見込んでいる分野」として、「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」、「セキュリティサービス関連」、「暗号技術」が上位に挙げられ、本調査はこれを反映したものとなっている。
- 企業について見ると、比較的取り組み割合が高い分野と低い分野に分けることができ、緩やかな「二極化」の傾向が見られる。

［比較的取り組み割合が高い分野］	［比較的取り組み割合が低い分野］
認証技術	暗号技術
ネットワークセキュリティ	不正侵入対策
セキュリティサービス関連	ウイルス対策

- 大学について見ると、ほぼ全ての分野において、同程度に実用化（製品化）されているが、その割合は低い。

【経年比較】

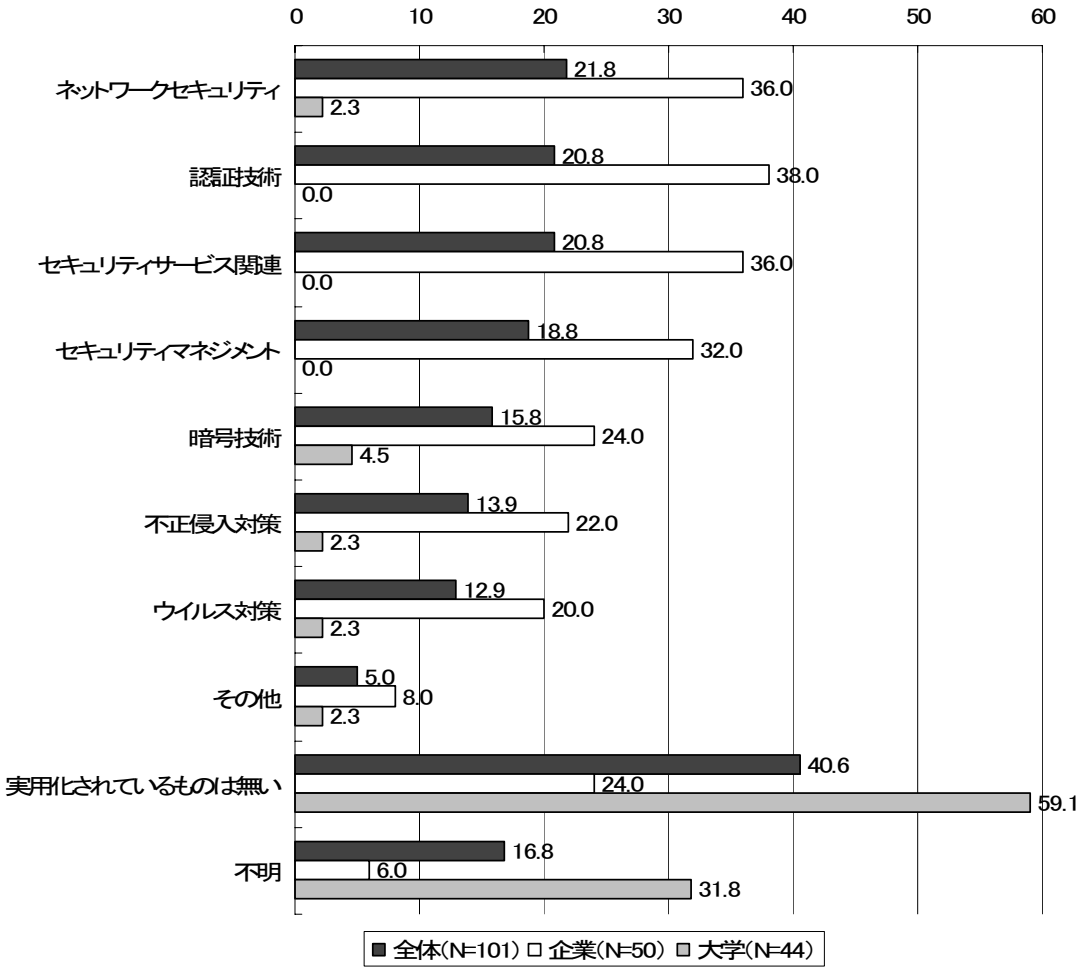
- 全体で見ると、「セキュリティサービス関連」および「ウイルス対策」が増加傾向にある。
- 企業では、「セキュリティサービス関連」、「ウイルス対策」および「ネットワークセキュリティ」が増加傾向にある。
- 大学では、「暗号技術」を始めとして、実用化（製品化）が緩やかに進むと思われるものの、実用化（製品化）されているアクセス制御機能が極めて少ない。

【本調査】

現在、実用化（製品化）されているアクセス制御機能を見ると、全体としては「ネットワークセキュリティ（２１．８％）」、「認証技術（２０．８％）」、「セキュリティサービス関連（２０．８％）」および「セキュリティマネジメント（１８．８％）」の割合が比較的高い。

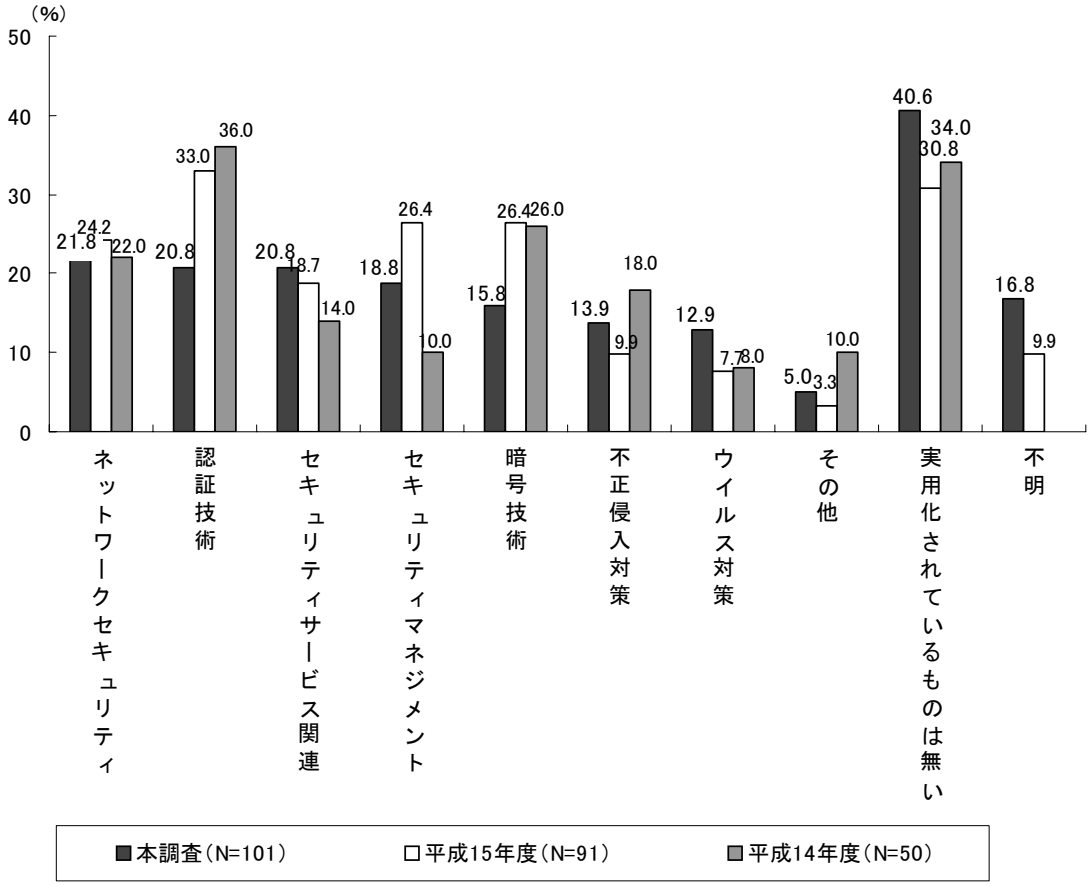
企業の特徴として、比較的取り組み割合が高い分野と低い分野に分けることができ、緩やかな「二極化」の傾向が見られる。

大学の特徴として、ほぼ全ての分野において、同程度に実用化（製品化）されているが、その割合は低い。



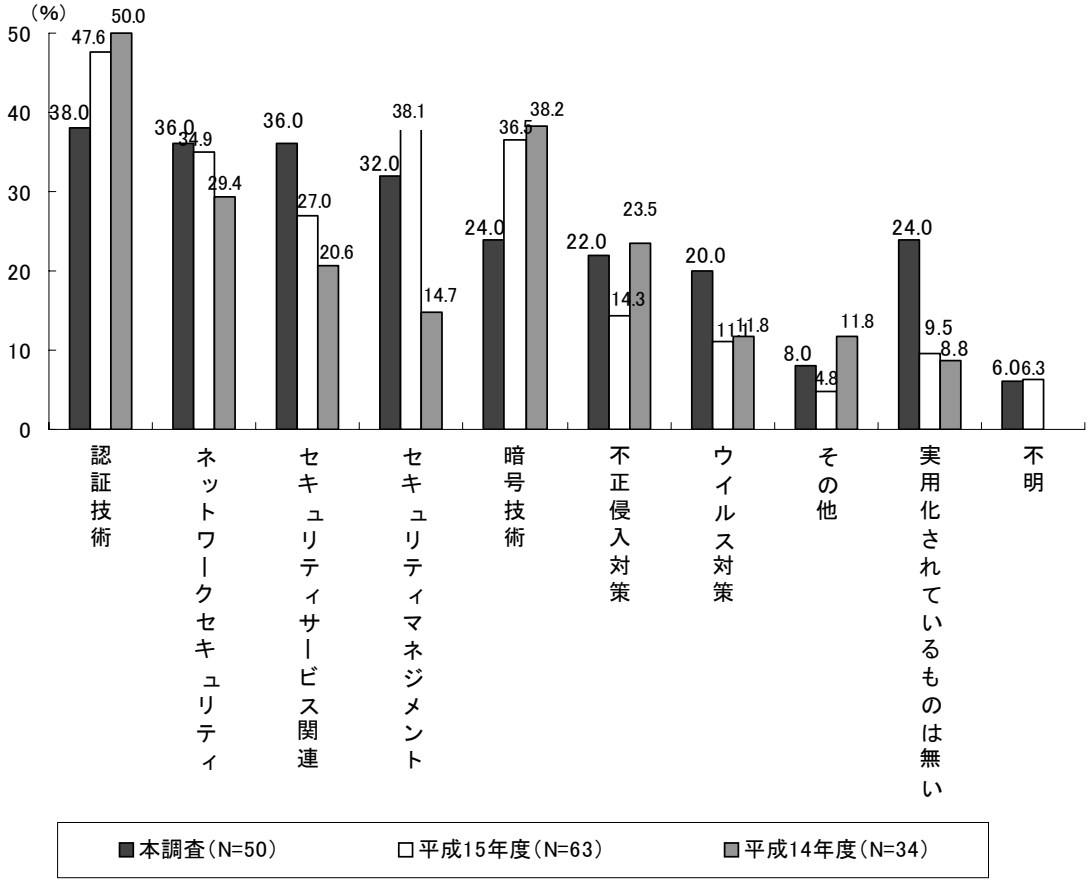
【経年比較（全体）】

平成１５年度調査と比較すると、「セキュリティサービス関連」および「ウイルス対策」が増加傾向にある。



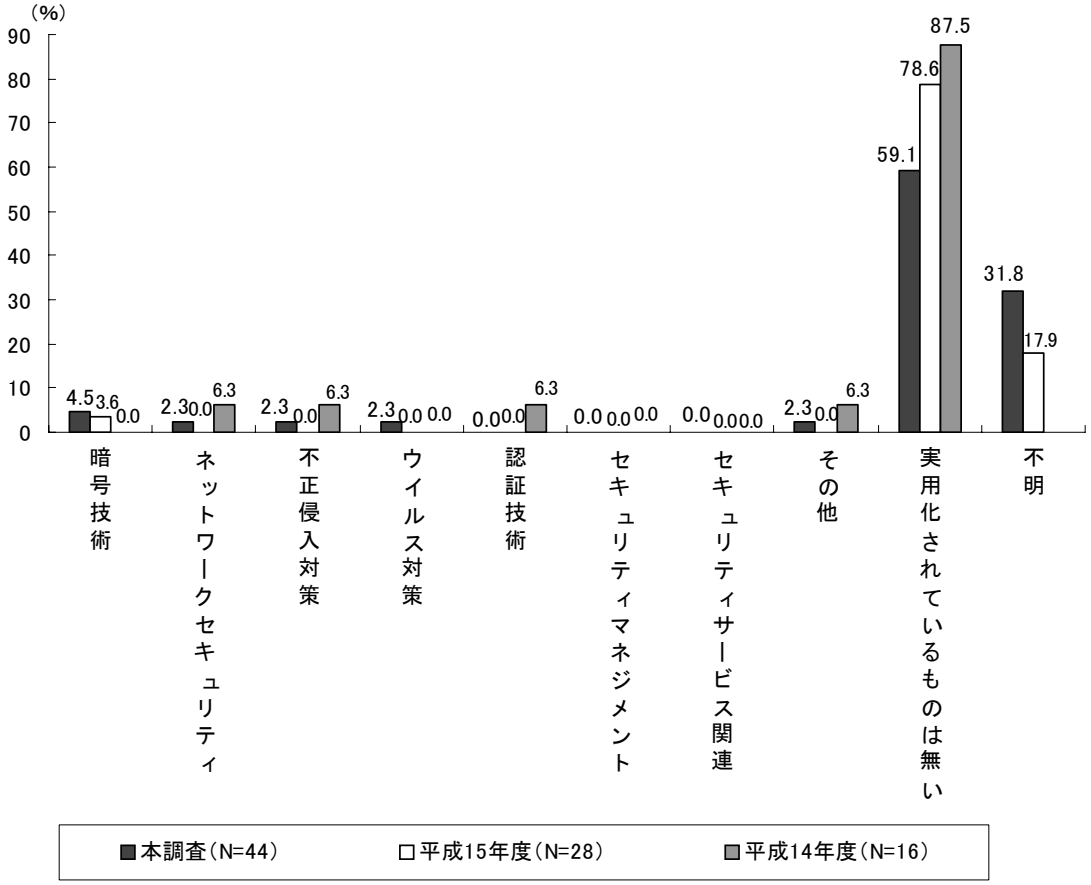
【経年比較（企業)】

平成１５年度調査と比較すると、「ネットワークセキュリティ」、「セキュリティサービス関連」および「ウイルス対策」が増加傾向にある。



【経年比較（大学)】

平成１５年度調査と比較すると、「暗号技術」を始めとして、実用化（製品化）が緩やかに進むと思われるものの、実用化（製品化）されているアクセス制御機能が極めて少ない。また、「セキュリティマネジメント」および「セキュリティサービス関連」は他の分野に比べると実用化（製品化）し難い分野とも言える。



1.6 今後、（実用化）製品化を見込んでいるアクセス制御技能

【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を見ると、全体としては「認証技術（１８．８%）」、「セキュリティマネジメント（１６．８%）」、「ネットワークセキュリティ（１５．８%）」および「セキュリティサービス関連（１５．８%）」の割合が比較的高い。
- 企業について見ると、比較的割合が高い分野と低い分野に分けることができ、緩やかな「二極化」の傾向が見られる。

［比較的割合が高い分野］	［比較的割合が低い分野］
認証技術	暗号技術
ネットワークセキュリティ	不正侵入対策
セキュリティマネジメント	ウイルス対策
セキュリティサービス関連	

- 大学について見ると、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「認証技術」の割合が比較的高いものの、企業に比べると極めて低い。また、「実用化の予定が無い」と回答した割合が高い。

【経年比較】

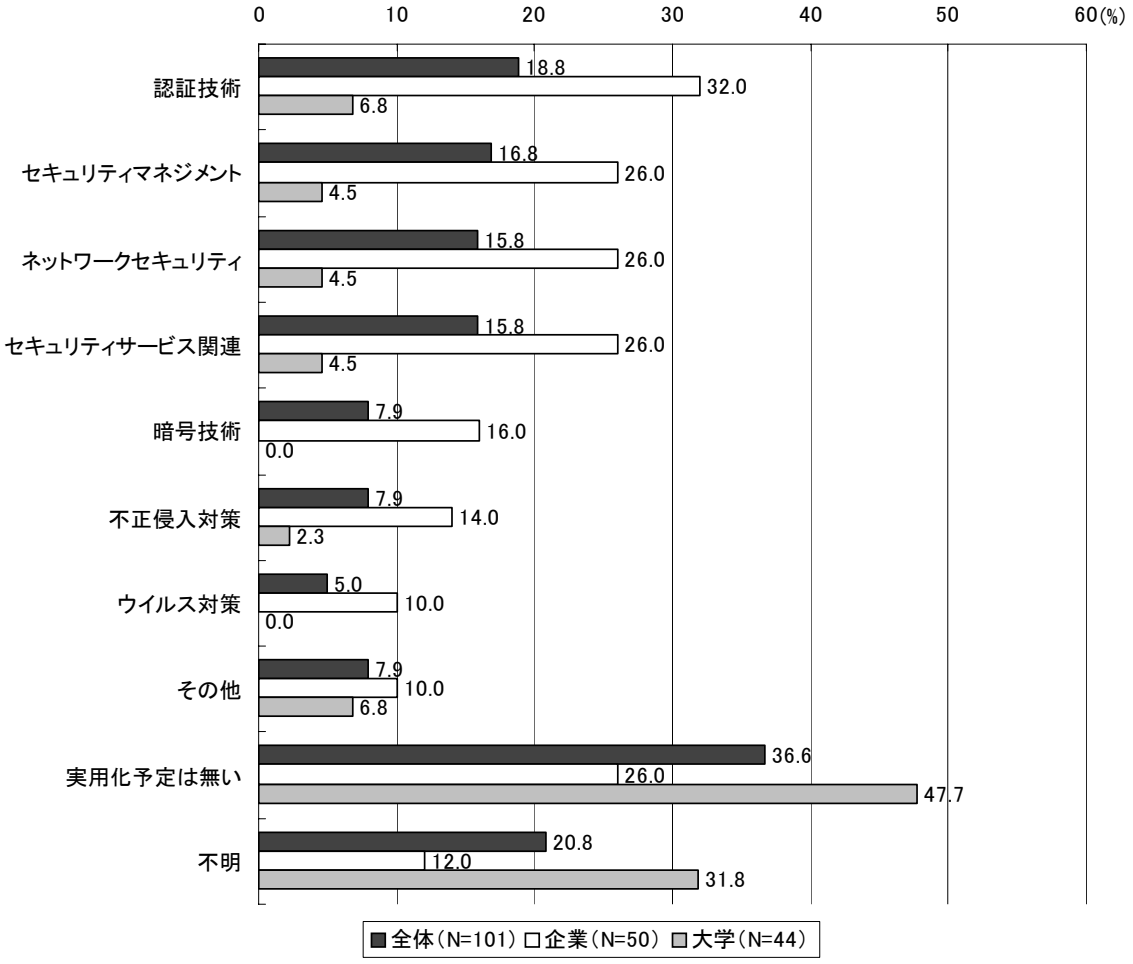
- 全体としては、「実用化予定は無い」の割合が高く、「不正侵入対策」を除く全ての分野で減少傾向にある。
- 企業では、「認証技術」および「不正侵入対策」が増加傾向にある。
- 大学では、「不正侵入対策」、「セキュリティマネジメント」および「セキュリティサービス関連」が増加傾向にある。

【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を見ると、全体としては「認証技術（１８．８％）」、「セキュリティマネジメント（１６．８％）」、「ネットワークセキュリティ（１５．８％）」および「セキュリティサービス関連（１５．８％）」の割合が比較的高い。

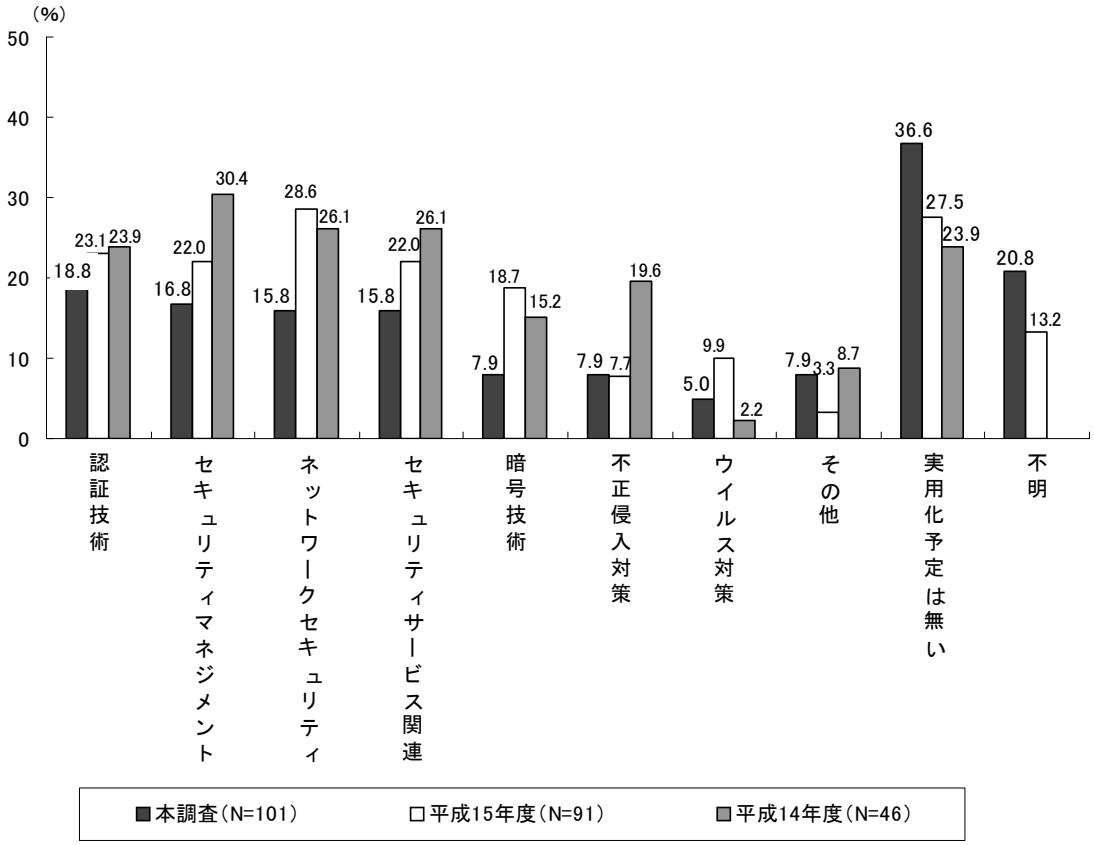
企業の特徴として、比較的割合が高い分野と低い分野に分けることができ、緩やかな「二極化」の傾向が見られる。

大学の特徴として、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「認証技術」の割合が比較的高いものの、企業に比べると低い。また、「実用化の予定が無い」と回答した割合が高い。



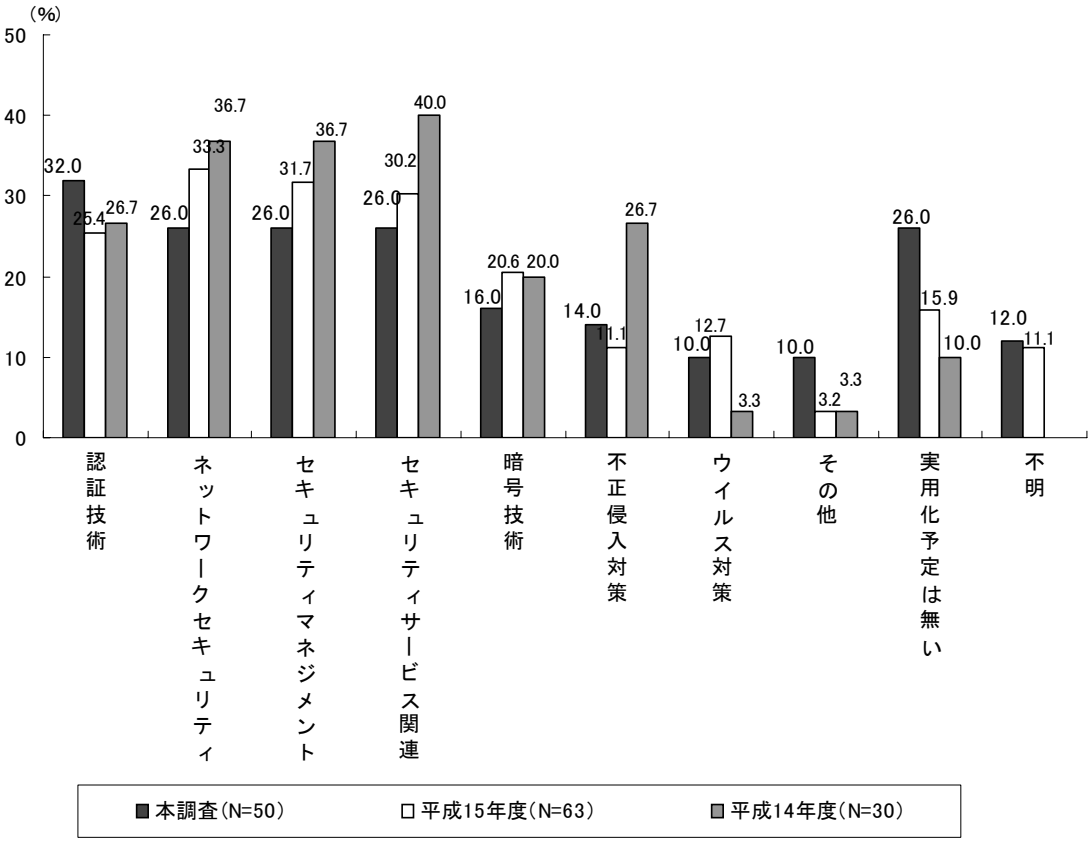
【経年比較（全体）】

平成１５年度調査と比較すると、「実用化予定は無い」の割合が高く、「不正侵入対策」を除く全ての分野で減少傾向にある。上位は関心の高い分野であるが、実用化の見通しが見えていない技術を創りだそうという試みも多いようである。



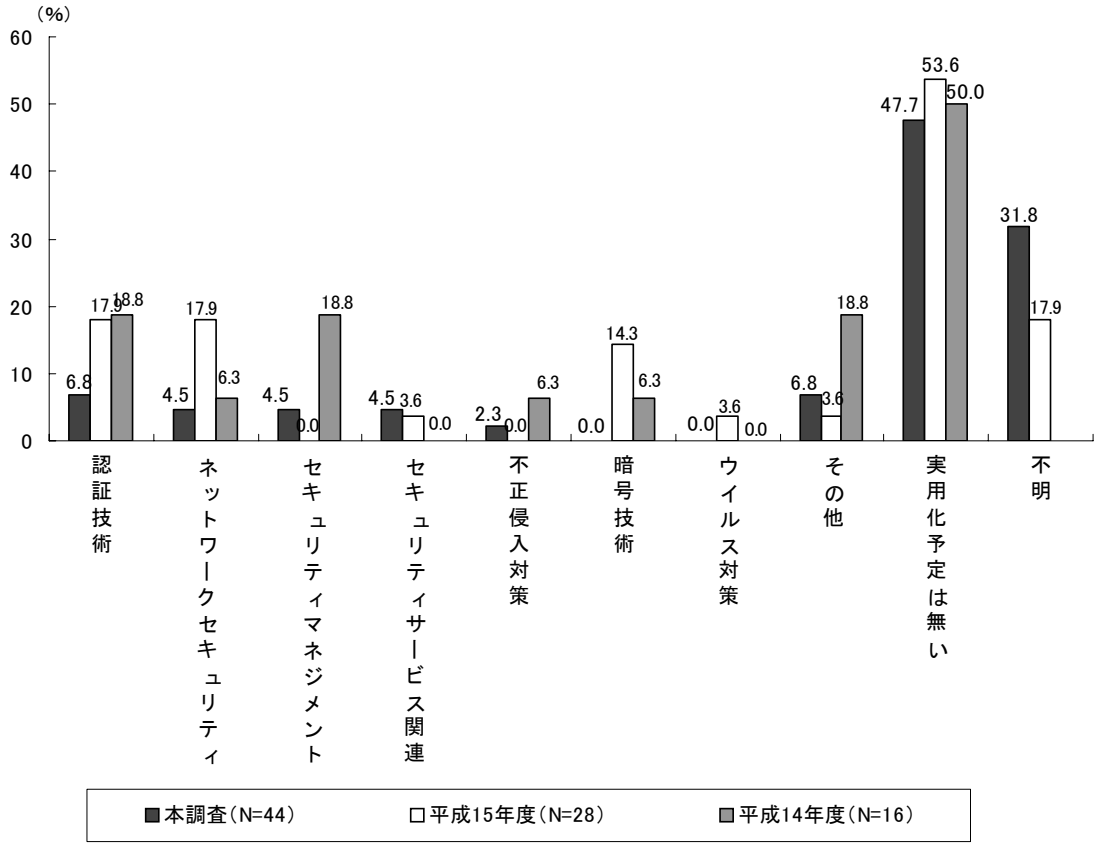
【経年比較（企業)】

平成１５年度調査と比較すると、「認証技術」および「不正侵入対策」が増加傾向にあるが、「認証技術」「ネットワークセキュリティ」「セキュリティマネジメント」「セキュリティサービス関連」が根強い人気を持っているようである。



【経年比較（大学)】

平成１５年度調査と比較すると、「不正侵入対策」、「セキュリティマネジメント」および「セキュリティサービス関連」が増加傾向にあるが、特に目立った変化は見られない。



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、解答をそのまま、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」

ネットワークを守る技術は、インターネット自身に対しては重要な位置付けにある。今回の調査でも大学や研究部門がいろいろな観点から試行を行っているようである。基礎研究分野が多いようであるが、現在までにわかってきているインターネットの問題点を解決するための方策をまとめ、実証実験を行い、国際標準へも提案して議論できるような成果が出てくることが望まれる。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
リコーテクノシステムズ株式会社	センター型検疫ネットワーク提供サービス 平成 16 年 10 月～ なし	・既要構成をまとめビジネスモデル特許出願準備中。 ・製品の技術検証中。 ・サポート体制模索中。
熊本大学 総合情報基盤センター	DNSクエリによるウイルス検知ならびに防御 平成 13 年～ なし	学内のネットワークで実証実験中。
中京大学	MTA による SPAM 対策システム 平成 15 年 11 月～ なし	RFC2821 を守らない SPAM を 100%拒否可能。
株式会社日立情報システムズ	SHIELD/ExLink(シールド/イーエクスリンク) 平成 16 年 10 月～17 年 9 月 今後作成予定	･各種のセキュリティ製品と連携し、セキュリティのインシデントを収集し、(ウイルス・ワーム感染、不正アクセス、情報漏えい、盗聴)セキュリティ運営ポリシーに基づいて、被害の拡大阻止のために各種セキュリティ製品と連携し防御する。(ファイアウォール、接続遮断装置)。 ・システム管理装置との連携。
株式会社日立情報システムズ	SHIELDeXpress i-monitor 平成 16 年 10 月～17 年 9 月 なし	セキュリティ脆弱性及びインシデントの情報を世界及びローカルから収集し、監視対象のサイトに迫る攻撃の脅威を分析する。 ・脅威分析の結果は管理者へ通知。 ・事前に指定された監視対象サイトのセキュリティ運用ポリシーに基づいて、防御処置の自動的な実施。

②「技術の実用化（製品化）状況」

ネットワークを守るということで、対象が大きいせいもあり、企業向けの製品が中心となっている。40 件（全回答者の 36.4%）という回答数は、この分野の需要が強いことが伺われる。回答内容の製品群を見ると、情報漏えいや証拠保全(フォレンジック)、監視サービスなどに関するものが多い。これらもコンシューマ向けではなく、エンタープライズ向けの製品・サービスが多い理由であろう。

開発元	製品名/発売時期/URL	概要・特徴など
三菱スペース・ソフトウェア株式会社	MSIESER(エム・シー・サー) 平成 15 年 2 月 14 日頃～ http://www.ryoyo.co.jp/product/system/msieser/index.html	概要：network の通信を記録し、必要なときに解析、復元して network 利用を監視します。また記録されたパケットメンテは暗号化され、原本性を確保し、法的証拠として企業の雇用を守ります。特徴：①優れた安全性（装置のセキュリティ機能）。記録されたデータはハッシュ値が付与され、暗号化されます。管理端末からの操作ログが記録されます。アクセス権限もシステム管理者、データ閲覧者、監査者に細分化されています。②自社は拡張性。記録装置は選択自由で大容量も対応しています。③既存のシステムに一切影響を与えません。スイッチのミラーポートからパケットを取得するためのnetworkへの負荷がかかりません。構成変更も必要ありません。
ファルシステムコンサルティング株式会社	Wise Point 平成 15 年 4 月 1 日頃～ http://wisepoint.jp/	Wise Pointの主な機能は独自方式の認証。Webアプリケーションに対するシングルサインオン、アクセスコントロール等の機能を持っております。特に認証方式については多種の認証方式（Jパスワード、マトリクスコード、イメージマトリクス、携帯電話ID認証）を持っております。
株式会社インテック	EINS/MSS+ 未定 http://www.intec.co.jp/service/network/einsmss.html	
リコーテクノシステムズ株式会社	ITSheriff AD・ST・LT 平成 15 年 7 月 4 日頃～ http://www.it-sheriff.jp/	ITSheriff Box（ファイアウォール）による外部攻撃侵入からのネットワーク保護。またウイルス対策を行ないます。監視センターから 24 時間 365 日 ITSheriff Box やお客様サーバ、ネットワーク機器を遠隔監視し、異常検出時の対応を行ないます。さらに月間の監視結果レポート・コンタクトセンターによるお客様対応窓口を提供します。
セキュアコンピューティングジャパン株式会社	Side Winder 平成 8 年～ http://www.sidewinder.jp	商用フィアウォールの草分け的存在であり、その一号機は平成 7 年の米国家安全保障局への納入実績を持つ。独自の Type enforcement （SE Linuxと同じ仕組み）と呼ばれる技術により、クラックが極めて困難なシステムを実現しており、発売以来、今だにクラックされた実績がない。またアプリケーションゲートウェイ方式をその最初のバージョンより採用しており、一般に「ファイアウォールで防げない」と言われる攻撃を防ぐのも特徴の一つである。

開発元	製品名/発売時期/URL	概要・特徴など
シスコシステムズ株式会社	Cisco PIX Security Appliance 未定 http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/pix/	強固なエンタープライズクラスのネットワークセキュリティサービスを実現する。ファイアウォール、VPN、侵入保護機器です。
シスコシステムズ株式会社	Cisco Intrusion Detction System 4200 センサ 未定 http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/ids4200/	ネットワーク全体に透過的な保護を提供可能で、ネットワークを通過する不正で悪意のある行為からネットワークを保護します。
株式会社シマンテック	Symantec Incident Manager 未定 http://www.symantec.com/region/jp/products/sim/	URL を参照。
株式会社シマンテック	Symantec Event Manager for Antivirus 未定 http://www.symantec.com/region/jp/enterprise/products.html/	URL を参照。
株式会社シマンテック	Symantec Gateway Security 300series 平成 16 年 8 月～ http://www.symantec.com/region/jp/products/sgs300/	URL を参照。
株式会社シマンテック	Symantec Gateway Security 5400series 平成 15 年 10 月～ http://www.symantec.com/region/jp/products/sgs/	URL を参照。
株式会社シマンテック	Symantec Network Security 7100series 平成 16 年 12 月～ http://www.symantec.com/region/jp/products/sns/	URL を参照。
株式会社シマンテック	Symantec Enterprise Firewall8.0 平成 16 年 6 月～ http://www.symantec.com/region/jp/products/sef/	Symantec Enterprise firewall は独自のハイブリットアーキテクチャを採用しており、企業ネットワークを様々なネットワーク攻撃力で不正なアクセスから強固に、そしてプロアクティブに保護し、企業の情報資産の活用と保護を促進します。主な機能 ・アプリケーションプロキシをそなえたフルインスペクション FW。 ・プロキシセキュアド VPN による安全性の高い IPSec VPN の提供。 ・クラスター構成による冗長化と負荷分散が可能。 ・Web ベースの容易な管理。
株式会社エス・エス・アイ・ジェイ	VAISインターネット脆弱性検査サービス 平成 16 年 6 月～	QualysGuard および Appscan を使用した2種類の脆弱性検査サービス。 ①N-VAISネットワーク脆弱性検査サービス。Qualys 社の QualysGuard による検査を行ない、平易な日本語で記述された判り易い形式でのレポートを提出するサービス。 ②W-VAIS Web アプリケーション脆弱性検査サービス。SANCTUM社の Appscan とエンジニアによる検査結果から脆弱性のリスク分析と対処法の詳細説明

開発元	製品名/発売時期/URL	概要・特徴など
	なし	など顧客向けにカスタマイズされたレポートを提出するサービス。
沖電気工業株式会社	異常トラフィック監視システム 平成 11 月 9 日頃～ http://www.oki.com/jp/Home/JIS/New/OKI-News/2004/11/z04093.html	異常トラフィック監視システムはトラフィックの状況を監視するプローブ装置と、プローブ装置を管理するマネージャ装置から構成され、最大8台までのプローブ装置を配置することができます。(製品はアプライアンスにて提供)異常トラフィック監視システムには、アプケーション別のトラフィック計測機能、異常トラフィック検出機能、アクション機能があり、ネットワークトラフィックの統計画面から簡易な操作でトラフィック調査が行えるだけでなく、ネットワーク感染型ワームの感染活動を検出することが可能です。本製品は Fast Ethernet 対応のスタンダードモデルと Gigabit Ethernet 対応のハイエンドモデルを揃えました。
コンピュータ・アソシエイツ株式会社	eTrust Access Control 未定 http://www.caj.co.jp/etrust/ac	サーバ上のリソース(ファイルやプログラム等)に対するアクセス制御を実現する製品。役割に応じた適切なアクセス権限を設定(適切なユーザに適切な権限を与える)ことが可能。正常アクセスも含む追跡可能な監査ログを取得する。“だれが”、“いつ”、“どの端末から”、“何のツールを使って”、“どのリソースへ”といった4W1Hに基づいたログを出力。ログは誰も改ざんできない仕組みとなっている。
コンピュータ・アソシエイツ株式会社	eTrust Secure Content Manager 未定 http://www.caj.co.jp/etrust/scm	迷惑メール、情報漏えい、e メールに起因する法的責任、ウイルス、悪意あるコンテンツ・プログラム、不快なコンテンツなど、様々な脅威からPCを保護する統合コンテンツセキュリティソリューション。ビジネス主導型ポリシーエンジン、機密情報のフィルタリング、警告とアクションの自動化、ポリシーの一元管理、迷惑メールとURLアクセスに関する独自のルール作成など、コンテンツセキュリティに重要な機能を豊富に備えている。
コンピュータ・アソシエイツ株式会社	eTrust Anti Virus 未定 http://www.caj.co.jp/etrust/antivirus/	サーバ、クライアントPC、グループウェア、ゲートウェイまでウイルスの脅威から保護するアンチウイルスソリューション。2つのウイルススキャニングエンジンでウイルスを完全ブロック。特に企業での利用を前提にして管理機能がすぐれており、運用や導入に大きなメリットとなる。
株式会社インテリジェントウェイブ	CWAT(Cyber Warning Alert Termination) 平成 15 年 11 月～	CWATはオーガナイゼーションモニタ(統合監視コンソール)、セグメントディフェンスコントローラ(ネットワーク監視)、アンノウンターミナルディフェンスコントローラ(未登録端末監視)、オペレーションディフェンスコントローラ(オペレ

開発元	製品名/発売時期/URL	概要・特徴など
	http://www.iwi.co.jp/japanese/cwat/news/index.html	ーション監視）で構成された内部情報漏洩対策システムです。CWATは、ネットワーク情報を監視するだけではなく、外部に持ち出されるモバイルPCやクライアントPCでのFD、CDへの書き出し、外部接続バス経由での未登録端末の直接接続も監視できる機能を持っています。更に、操作員のポリシーに違反した挙動や、普段と著しく異なった挙動を監視することができます。
トップレイヤーネットワークスジャパン株式会社	Attack Mitigator IPS 平成 14 年 3 月～ http://www.TopLayer.co.jp/products/ol_attack.html	Attack Mitigator IPSは、不正アクセスや、悪意のあるコンテンツ（ウイルスやワーム、トロイの木馬その他）及び DoS/DDoS などの量的な攻撃からネットワーク・レベルおよびアプリケーションレベルでの最適なサービスプロテクションを提供する。TipFireTMASICとTopinspectTM詳細パケット分析アルゴリズムによるハイパフォーマンスなアプリケーション使用基準検査により、重要サーバに対する各種のサイバー攻撃を検知および遮断を行い、サーバに脆弱性が内包されている場合も不正侵入を未然に防ぐ
トップレイヤーネットワークスジャパン株式会社	Secure Controller 平成 16 年 6 月～ http://www.TopLayer.co.jp/products/02_sec.html	Secure Controllerは、ユーザ認証とvZONE機能によるアクセス制御とポリシーベースのQoSを提供。クオリティ株式会社および株式会社PFUが提供するソフトウェアとの組み合わせによりSPCソリューション（PCプロファイル認証および検疫）ネットワークを実現。ブリッジ型の機器であり、既存ネットワークの構成変更は不要である。
横河電機株式会社	As－C/h、As－C/m、As－F 平成 15 年 8 月 26 日頃～ http://www.yokogawa.co.jp/itbiz/as/	IEEE802.1XとRADIUS認証ソフトウェアを搭載したアプライアンス製品。IEEE802.1Xは、有線認証スイッチと無線LANに、RADIUSは電話回線（RAS）にクライアントPCを接続する時の認証プロトコルの規定です。これらを搭載するASシリーズは、As－C／h、As－C/m、As－Fの3機種より構成されます。これらは、EAP－TLS、EAP－TTLS、PEAPの認証プロトコルに対応しています。As－C/h、As－C/mでは認証ソフトウェアを加えてCA機能を搭載しデジタル証明書を発行することが可能です。外部のLDAPサーバとの連携も可能です。As－Fは、小型で駆動部がバッテリバックアップ機能を搭載し小規模オフィスや支社支店や各フロアエッジへの配置が可能です。As－Cをセンターに配置し、PROXYよりエッジに配置したAs－Fと分散構成をとることが可能です。
マカフィー株式会社	IntruShield 平成 15 年 10 月 1 日頃～ http://www.mcafee.com/jp	〈IntruShield〉システムの脆弱性を狙った攻撃や侵入、MSプラスト、Sasserの様なワームおよび DoS 攻撃に対して、高精度の検知とリアルタイムの防御が可能です。これらの攻撃に対して、予防、被害拡大の防止、問題発生時の適切な対応のための情報提供により、高度なセキュリティを実現します。
マカフィー株式会社	WebShieldAppliance 平成 13 年 8 月 15 日頃～	＜WS＞McAfee WebShield Appliance v3.0 は、容易に設定できるインターネットゲート

開発元	製品名/発売時期/URL	概要・特徴など
	http://www.mcafee.com/jp	ウェイのためのソリューションで、SMTP、HTTP、FTP、およびPOPプロトコルの受信・送信トラフィックをスキャンします。比類のないパフォーマンスとウイルスの検知・駆除機能を提供し、あらゆる規模の企業にとって無用なスパム形式のメールや迷惑なコンテンツを防止します。スパイウェアやアドウェア、増加が著しいフィッシングメールなどにも幅広く対応する製品です。
サン・マイクロシステムズ株式会社	Sun Ray 平成 11 年 9 月 20 日頃～ http://jp.sun.com/products/desktop/infoappliances/	Sun Ray Appliance は、完全にステートレスで管理の必要がないクライアント– アプライアンスです。そこでは、キーボードなどの入力や画面へのピクセル（画素）の表示のみを行い、すべてのアプリケーションの処理やオペレーティングシステムの動作、データの保存は全てサーバ側で行われます。ユーザは、シンプルな環境のもとで作業を行うことができます。また、あらゆる資源がサーバ側に集約されているため、システム管理者は集中管理を行うことができます。信頼性やスケーラビリティの高い環境を利用できるのも、Sun Ray Appliance環境の魅力です。Sun Ray Applianceはデータや状態を一切保持していないステートレスな端末なので、必要な際には簡単に他のアプライアンスと交換をすることができます。 – 豊富なマルチメディア機能 – より低いTCO（Total Cost of Ownership / 総合所有コスト）、より低い管理コスト –Hot Desking によるセッションの可搬性 – 総合面で優れた管理性 – そして「デスクトップマシンのアップグレードは一切不要」
サン・マイクロシステムズ株式会社	SunScreen Secure Net 未定 http://jp.sun.com/software/security/securenet/	SunScreen Netは、アクセス制御や、認証、ネットデータの暗号化などを行う汎用的な全社向けファイアウォールシステムです。SunScreen Secure Netには、ネットワークのアクセス制御を行うルールベースの動的なパケットフィルタリングエンジンと暗号化/認証エンジンがあります。暗号化/認証エンジンに公開鍵暗号化技術を統合することにより、安全な仮想プライベートネットワーク（VPN）ゲートウェイを作成できます。
サン・マイクロシステムズ株式会社	Trusted Solaris 未定 http://jp.sun.com/software/solaris/trustedsolaris/	高レベルのプライバシー、追跡可能性の向上、セキュリティ違反リスクの軽減を実現し、政府関係機関、情報関係機関、およびセキュリティ関係機関での実績を持ち、金融、健康管理、小売などの業界で足場を固めたTrusted Solaris Operating System（OS）は、商用グレードのOSへのセキュリティの組み込みを実現します。Trusted Solaris OSを使用することによって、デスクトップユーザからデータセンターのユーザまでが、ネットワークのセキュリティリスクを軽減し、セキュリティの信頼性をさらに高めることができます。

開発元	製品名/発売時期/URL	概要・特徴など
サン・マイクロシステムズ株式会社	Solaris 10 未定 http://jp.sun.com/software/solaris/trustedsolaris/	Solaris 10 はエンタープライズを異なったレベルで保護できる。先進的なセキュリティ機能を備えています。このセキュリティシステムは、外部からの悪意を持ったアタックや、内部からの不正なデータアクセスを防ぎます。再設計された暗号化フレームワークは、ハードウェアによる暗号化が可能な場合は自動的にそれを選択することで最適な暗号化メソドを選択し、柔軟な管理を実現します。Process Rights Managementコンポーネントが、どのユーザをどのプロセスに対し、何時、どのような権限を与えるのか詳細な制御を可能にします。
サン・マイクロシステムズ株式会社	Sun Crypto Accelerator 未定 http://jp.sun.com/products/networking/sslaccel/	Sun Crypto AcceleratorはEコマース等で標準的に使用されるSSL トランザクション処理を高速化するPCI拡張カードです。Sun Crypto Accelerator1000は、SSL計算処理専用のコプロセッサとして動作し、SSL処理をホストCPUから切り離し(CPUオフロード)ホストCPUの負荷を軽減します。
サン・マイクロシステムズ株式会社	Sun Fire B10p 未定 http://jp.sun.com/products/networking/blades/ssl/	Sun Fire B10p SSLプロキシ・ブレードは、Sun Fireブレードプラットフォームの構成要素として、物理的にも機能的にもシームレスに統合されます。SSLオフローディングのためにカスタムASICとファームウェアで実装されたSun Fire B10p SSLプロキシ・ブレードは、それぞれのサーバのホストCPUによるSSL処理と比較して、最大10倍のSSLトランザクション処理能力を提供します。同時に、ホストCPUのすべてのリソースを、本来のサービス提供に利用できるようになります。
サン・マイクロシステムズ株式会社	Sun N2000 Series Secure Application Switch 未定 http://jp.sun.com/products/networking/n2000/	Sun N2000 Series Secure Application Switchは、効率的なリソース運用/サービス統合/先進のコスト・パフォーマンスで、企業のセキュアなネットワーク・コンピューティング環境構築に伴うコストの複雑性を解消します。Sun N2000 Series Secure Application Switchには、ワイヤ・スピードGigabitアプリケーション・スイッチ/チップ・レベルの組込みセキュリティ/リソースの動的な仮想化技術が統合されています。一つのシステムにこれら技術が統合されているので、既存サーバの負荷分散/SSLの高速化/帯域幅管理などを実現するために、アプライアンスなど独自機能を提供する高価なコンポーネントを必要とせず、大幅なTCO削減や分散型コンピューティング環境の管理を簡素化します。
サイバーソリューション株式会社	CYBER－SPACE 平成 13 年 2 月～ http://www.cybersolution.co.jp	・IDCと監視。 ・ネットワーク(Global, Private), サーバの死活、状態監視と対応(ディスパッチレベル) ・ウイルス対応状況の監視と通知。・情報漏えい監視ツールの販売。
広島大学 情報メディア教育センター	FEREC 平成 16 年 2 月～ http://www.ferec.jp	大学内等において認証付情報コンセント機能を手軽に提供する。本製品は広島大学が独自に研究・開発した PortGuard システムのコンセプトを元に、(株)ネットスプリングにて開発した製品である。

開発元	製品名/発売時期/URL	概要・特徴など
富士通株式会社	Interstage Security Director 平成 12 年 7 月 17 日頃～ http://interstage.fujitsu.com/jp/v6/sd	本製品はインターネット上でサービスを提供する www サーバやアプリケーションサーバのためにセキュリティを確保する製品です。ファイアウォール機能およびアプリケーションゲートウェイ機能（HTTP アプリケーションゲートウェイ機能/OP アプリケーションケートウェイ機能）により不正アクセスの防止、通信データの保護、ユーザ認証、内部サーバの隠蔽等を含む強固なセキュリティソリューションを提供します。携帯端末(I モード）からのアクセスについては、登録された端末のみアクセスを許可することで、セキュリティ強度を高める事も可能
富士通株式会社	Safeauthor 平成 9 年 2 月末日から http://software.fujitsu.com/jp/linax/products/software/safeauthor/	概要：ユーザ認証、課金情報を管理する RADIUS サーバ製品。 特徴：・無線 LAN 認証(IEEE802.1xEAP)に対応。 ・EAP-MDG,EAP-TLS,EAP-TTLS,EAP-PEAP に対応。 ・認証 DB ひとつで LAN とリモートアクセスユーザを集中管理。 ・リモートアクセスユーザへの IP アドレスの自動割当。 ・Radius-Proxy による負荷分散 ・Web ブラウザを利用した容易な環境設定が可能。 ・マルチベンダ Radius クライアント対応。
富士通株式会社	セキュリティ監視サービス 平成 12 年 9 月 5 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	富士通の SOC：「富士通 IT マネージメントセンタ」より、お客様インターネットサイトを 24 時間 365 日監視し、クラッカーによる不正アクセスに迅速に対応します。また、監視状況を集計・分析して月報（Web 等）を提供します。
富士通株式会社	ファイアウォール運用サービス 平成 15 年 2 月 6 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	お客様の運用に合わせたファイアウォールの最適な設計、構築と 24 時間 365 日監視・障害対応体制の提供により、ファイアウォール運用におけるお客様の負担を大幅に削減する。
富士通株式会社	Web アプリケーションセキュリティ診断サービス 平成 16 年 6 月 23 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	診断ツールと富士通独自ノウハウで、インフラ・OS・ミドルウェアを診断するサーバスキャンでは対応していない、お客様固有開発の Web アプリケーションの脆弱性を診断・評価・分析し、その危険性と具体的な対策指針をご提供します。
富士通株式会社	エンドポイントセキュリティサービス 平成 16 年 6 月 4 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	システム利用者の運用に Windows セキュリティ修正プログラムの適用やウイルスパターンファイルの更新などのセキュリティ対策をシステムで統合管理する環境をご提供します。
株式会社日立情報システムズ	PKI 認証基盤　SSCom（エスエスコム） 平成 11 年 5 月頃～ http://www.shield.ne.jp/products/sscom/index.html	認証機能とアクセス制御機能を組み合わせた認証基盤ソフトウェア。 特徴： ・Felica、PUPPY、認証トークン、IC カード等の認証媒体を使用し安全な認証を実現。 ・VPN 通信機能により盗聴や改ざんから通信内容を保護。 ・グループアクセス制御による情報アクセス制御。

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 11 件（全回答者の 41.4%）と次のクライアント(PC)に次ぐ件数となっているが、これもサーバを取り巻くいろいろな脆弱性や不正アクセスの脅威から守らなければならないという問題意識が反映しているものと思われる。研究機関としては、やはり大学が多いのも、ネットワークと共通した傾向である。しかも、だいぶ具体的なテーマを持って研究を進めているところが多いようである。実用化（製品化）が近いものが多いのかもしれない。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
リコーテクノシステムズ株式会社	センター型検疫ネットワーク提供サービス 平成 16 年 10 月～ なし	・既要構成をまとめビジネスモデル特許出願準備中。 ・製品の技術検証中。 ・サポート体制模索中。
中京大学	MTAによるSpam対策システム 平成 15 年 11 月～ なし	RFC2821を守らないSpamを100%拒否可能。
日立ソフトウェアエンジニアリング株式会社	秘文 Advanced Edition 平成 11 年 1 月～19 年 12 月 http://hitachisoft.Jp/hibun/	
NEC ネクサソリューションズ株式会社	セキュリティ統合型アプライアンスサーバ用ソフトウェアの開発 平成 16 年 12 月 1 日～18 年 2 月 28 日 なし	セキュリティ統合型アプライアンスサーバの研究開発。主な目的は情報漏えいの防止／抑止。保護対象は社内、外を問わず公開されたWebサーバ。HTTP プロトコルに特化したアプリケーションレイヤーフォレンジックシステム。当該アプライアンスサーバはGatewayとして機能し、保護対象のサーバが接続されたネットワークに設置される。 ・データアクセスフォレンジック・・・全てのHTTPログと認証ログを保存、不正アクセスフィルタと連携し、怪しいアクセスログを別途保存。 ・認証フィルタ・・・誰がアクセスしたかを管理する。 ・不正アクセス防御フィルタ・・・SOIVDEFENCEの技術を転用して、不正な挙動を学習する機能強化。 ・リバースプロキシフィルタ・・・Gatewayとして動作させる。
弘前大学	Intrusion Detection Logic 平成 16 年 4 月～18 年 3 月 なし	論理設計中。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
宮崎大学	キーボード入力の監視による不正利用者発見システムの開発　平成 13 年 11 月 1 日～ 平成 13 年 11 月 1 日～ なし	なりすましによる不正利用者を発見することが本システムの目的です。利用者がキーボード入力を行っている様子を常に監視し、その特長を捉え、過去にその利用者が行ったキーボード入力の特徴と比較し、不正利用者か否かを判別し不正利用者を発見するシステムです。対象のOSはUNIXですが、Windows 上での監視システムの構築も検討中です。
宮崎大学	キーボード入力の監視による不正利用者発見システムの開発 平成 16 年 4 月 1 日～18 年 3 月 31 日 なし	コンピュータ（Windows）の不適切な使用を検知し、不正な操作を抑止することが本システムの目的です。Windows の利用者がキーボード入力を行なっている様子やアプリケーションの起動状況を常に監視し、不適切な文字入力やアプリケーションを起動した際には、その様子をコンピュータの管理者へ自動で連絡し警告を発するシステムです。インターネット上に設置された掲示板などへの不適切な書き込みを行なおうとした際や、違法もしくは違法性の高いソフトの実行を試みる際には、自動でネットワークの切断、コンピュータのシャットダウンを行うことで不適切な使用を抑止し、有害情報へのアクセスやネットワーク犯罪を防止する効果が期待できます。これまでに、Windows 上で入力した文字列や起動したアプリケーションの情報を取得できる監視ソフトのプロトタイプを開発しました。現在は、不適切な操作か否かを判別するアルゴリズムを開発中です。導入先としましては、主に教育機関や一般家庭において子供（未成年）が利用しているコンピュータなどに導入されることを期待しています。企業や自治体での導入におきましては、オペレーションの監視による機密情報の漏洩など、その他の不正な操作の防止に効果を発揮することが期待されます。
広島大学 情報メディア教育研究センター	脆弱性診断支援ツール 平成 15 年 4 月～ なし	大学等、比較的オープンな環境においては、ネットワークに接続されるサーバやクライアントのセキュリティ脆弱性（OS のパッチ等）の管理が非常に困難である。そのため、組織内の監視センター等からネットワークに接続されたサーバやクライアントに対し、脆弱性診断を行い、問題が発見されたマシンの管理者に対し、警告を出す事になるが、大規模な大学等では、必ずしも効果がない。本システムでは大規模組織の一部を管理する管理者が、脆弱性診断を利用し易くする機能等を提供する。
株式会社日立情報システムズ	SHIELD/ExLink(シールド/イーエクスリンク) 平成 16 年 10 月～17 年 9 月 今後作成予定	･各種のセキュリティ製品と連携し、セキュリティのインシデントを収集し、（ウイルス・ワーム感染、不正アクセス、情報漏えい、盗聴）セキュリティ運営ポリシーに基づいて、被害の拡大阻止のために各種セキュリティ製品と連携し防御する。（ファイアウォール、接続遮断装置）。 ・システム管理装置との連携。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
株式会社日立情報システムズ	SHIELDeXpress i-monitor 平成 16 年 10 月～17 年 9 月 なし	セキュリティ脆弱性及びインシデントの情報を世界及びローカルから収集し、監視対象のサイトに迫る攻撃の脅威を分析する。 ・脅威分析の結果は管理者へ通知。 ・事前に指定された監視対象サイトのセキュリティ運用ポリシーに基づいて、防御処置の自動的な実施。

②「技術の実用化（製品化）状況」

サーバ用の製品は、回答数 54 件(全回答者の 47.3%)を占め、最も多かった。製品内容も多様であり、いろいろな業務や用途に向けた製品が作られている。サーバを守るということで、ターゲットはエンタープライズレベルであるが、さまざまな規模を考えたものや、クライアント(PC)との連携や協調動作を前提にしたものもある。

今回の調査では、「セキュア OS」関係は回答数こそ少なかったが、今後、重要インフラ用のサーバを中心に、利用が増えてくると思われる。サーバへの認証やアクセス制御の考え方も、今までの方法論が変化してくることが予想される。必要であればこのような方法論も研究し利用する価値があるだろう。

不正アクセスを検出し防御する「アクセス制御製品」としては、サーバ向け製品が中核をなす。この意味でも種類、機能、規模など、多様な製品が提供されている。実際にアクセス制御を考える際には、この他にも多くの製品が存在しているので、十分に調査されることを勧める。

開発元	製品名/発売時期/URL	概要・特徴など
ジェイズ・コミュニケーション株式会社	Trustream 平成 16 年 7 月 1 日頃～ http://www.jscom.co.jp/trustream/index.htm	外部より侵入するウイルスから企業LANを守るための包括的高速アンチウイルスゲートウェイサーバであり、フィンランドのエフ・セキュア社からソフト提供を受け開発いたしました。
ファルシステムコンサルティング株式会社	Wise Point 平成 15 年 4 月 1 日頃～ http://wisepoint.jp/	Wise Pontの主な機能は独自方式の認証。Webアプリケーションに対するシングルサインオン、アクセスコントロール等の機能を持っております。特に認証方式については多種の認証方式（Jパスワード、マトリクスコード、イメージマトリクス、携帯電話ID認証）を持っております。
株式会社インテック	EINS/MSS+ 未定 http://www.intec.co.jp/service/network/einsmss.html	なし
リコーテクノシステムズ株式会社	ITSheriff AD・ST・LT 平成 15 年 7 月 4 日頃～ http://www.it-sheriff.jp/	ITSheriff Box（ファイアウォール）による外部攻撃侵入からのネットワーク保護。またウイルス対策を行ないます。監視センターから 24 時間 365 日 ITSheriff Box やお客様サーバ、ネットワーク機器を遠隔監視し、異常検出時の対応を行ないます。さらに月間の監視結果レポート・コンタクトセンターによるお客様対応窓口を提供します。
セキュアコンピューティングジャパン株式会社	Safe Word 平成 3 年～ http://www.safeword.jp	ワンタイムパスワードの草分け的存在であり、日本でも 10 年以上の間に渡る販売実績を持つ。独特の回数同期式と呼ばれる方式によって、時間同期式を採用している他社製品のユーザが悩まされるような時間のずれがないのが、最大の特徴である。
シスコシステムズ株式会社	Cisco Plx Security Appliance 未定 http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/pix/	強固なエンタープライズクラスのネットワークセキュリティサービスを実現する。ファイアウォール、VPN、侵入保護機器です。

開発元	製品名/発売時期/URL	概要・特徴など
シスコシステムズ株式会社	Cisco Intrusion Detction System 4200 センサ 未定 http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/ids4200/	ネットワーク全体に透過的な保護を提供可能で、ネットワークを通過する不正で悪意のある行為からネットワークを保護します。
シスコシステムズ株式会社	Cisco Security Agent 未定 http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/csa/	CSA はエンドユーザとも呼ばれるサーバおよびクライアントコンピュータに、侵入保護の機能を提供します。
株式会社シマンテック	Symantec Incident Manager 未定 http://www.symantec.com/region/jp/products/sim/	URL を参照。
株式会社シマンテック	Symantec Enterprise Security manager5.5 未定 http://www.symantec.com/region/jp/products/esm/	URL を参照。
株式会社シマンテック	Symantec Event Manager for Antivirus 未定 http://www.symantec.com/region/jp/enterprise/products.html/	URL を参照。
株式会社シマンテック	Symantec Mail Security for Domino on Windows 2000/2003 平成 16 年 6 月～ http://www.symantec.com/region/jp/products/sws notes/ http://www.symantec.com/region/jp/products/sws mse/ http://www.symantec.com/region/jp/products/sws smtp/	URL を参照下さい。
株式会社シマンテック	Symantec AntiVirus Corporate Edition 平成 16 年 6 月～ http://www.symantec.com/region/jp/enterprise/products.html/	URL を参照下さい。
株式会社シマンテック	Symantec Enterprise Firewall8.0 平成 16 年 6 月～ http://www.symantec.com/region/jp/products/sef/	Symantec Enterprise firewall は独自のハイブリットアーキテクチャを採用しており、企業ネットワークを様々なネットワーク攻撃力で不正なアクセスから強固に、そしてプロアクティブに保護し、企業の情報資産の活用と保護を促進します。主な機能 ・アプリケーションプロキシをそなえたフルインスペクション FW。 ・プロキシセキュアド VPN による安全性の高い IPSec VPN の提供。 ・クラスタ構成による冗長化と負荷分散が可能。 ・Web ベースの容易な管理。

開発元	製品名/発売時期/URL	概要・特徴など
サン・マイクロシステムズ株式会社	Sun Ray 平成 11 年 9 月 20 日頃～ http://jp.sun.com/products/desktop/infoappliances/	Sun Ray Appliance は、完全にステートレスで管理の必要がないクライアント- アプライアンスです。そこでは、キーボードなどの入力や画面へのピクセル(画素)の表示のみを行い、すべてのアプリケーションの処理やオペレーティングシステムの動作、データの保存は全てサーバ側で行われます。ユーザは、シンプルな環境のもとで作業を行うことができます。また、あらゆる資源がサーバ側に集約されているため、システム管理者は集中管理を行うことができます。信頼性やスケーラビリティの高い環境を利用できるのも、Sun Ray Appliance環境の魅力です。Sun Ray Applianceはデータや状態を一切保持していないステートレスな端末なので、必要な際には簡単に他のアプライアンスと交換をすることができます。 - 豊富なマルチメディア機能 - より低いTCO(Total Cost of Ownership / 総合所有コスト)、より低い管理コスト -Hot Desking によるセッションの可搬性 - 総合面で優れた管理性 - そして「デスクトップマシンのアップグレードは一切不要」
株式会社エス・エス・アイ・ジェイ	VAISインターネット脆弱性検査サービス 平成 16 年 6 月～ なし	QualysGuard および Appscan を使用した2種類の脆弱性検査サービス。 ①N-VAISネットワーク脆弱性検査サービス。Qualys 社の QualysGuard による検査を行ない、平易な日本語で記述された判り易い形式でのレポートを提出するサービス。 ②W-VAIS Web アプリケーション脆弱性検査サービス。SANCTUM社の Appscan とエンジニアによる検査結果から脆弱性のリスク分析と対処法の詳細説明など顧客向けにカスタマイズされたレポートを提出するサービス。
沖電気工業株式会社	異常トラフィック監視システム 平成 11 月 9 日頃～ http://www.oki.com/jp/Home/JIS/New/OKI-News/2004/11/z04093.html	異常トラフィック監視システムはトラフィックの状況を監視するプローブ装置と、プローブ装置を管理するマネージャ装置から構成され、最大8台までのプローブ装置を配置することができます。(製品はアプライアンスにて提供)異常トラフィック監視システムには、アプケーション別のトラフィック計測機能、異常トラフィック検出機能、アクション機能があり、ネットワークトラフィックの統計画面から簡易な操作でトラフィック調査が行えるだけでなく、ネットワーク感染型ワームの感染活動を検出することが可能です。本製品は Fast Ethernet 対応のスタンダードモデルと Gigabit Ethernet 対応のハイエンドモデルを揃えました。
沖電気工業株式会社	e すぷりっと便 平成 16 年 11 月頃～ http://www.oki.com/jp/NBC/netbiz/e_supu.html	「e すぷりっと便」は企業内外を問わず、電子メールや CD-ROM などのメディア形式で受け渡しされている個人情報・機密情報を紛失・盗難から守ります。情報は紛失や盗難が発生した場合、たとえ暗号化されていても情報流失と見なされます。「e すぷりっと便」は大事な情報を秘密分散法(電子割符)により、分割・暗号化し、異なる経路で相手に配送することで安全・確実な情報配送を実現します。

開発元	製品名/発売時期/URL	概要・特徴など
セコムトラストネット株式会社	セコム情報金庫 未定 http://www.secomtrust.net/service/s_product/kinko.html	ユーザサイトに設置する小型データセンター。高品質部材のメーカー等を中心に導入が進んでいる。
コンピュータ・アソシエイツ株式会社	eTrust Access Control 未定 http://www.caj.co.jp/etrust/ac	サーバ上のリソース(ファイルやプログラム等)に対するアクセス制御を実現する製品。役割に応じた適切なアクセス権限を設定(適切なユーザに適切な権限を与える)ことが可能。正常アクセスも含む追跡可能な監査ログを取得する。“だれが”、“いつ”、“どの端末から”、“何のツールを使って”、“どのリソースへ”といった4W1Hに基づいたログを出力。ログは誰も改ざんできない仕組みとなっている。
コンピュータ・アソシエイツ株式会社	eTrust Secure Content Manager 未定 http://www.caj.co.jp/etrust/scm	迷惑メール、情報漏えい、e メールに起因する法的責任、ウイルス、悪意あるコンテンツ・プログラム、不快なコンテンツなど、様々な脅威からPCを保護する統合コンテンツセキュリティソリューション。ビジネス主導型ポリシーエンジン、機密情報のフィルタリング、警告とアクションの自動化、ポリシーの一元管理、迷惑メールとURLアクセスに関する独自のルール作成など、コンテンツセキュリティに重要な機能を豊富に備えている。
コンピュータ・アソシエイツ株式会社	eTrust Pest Ptrol 平成 17 年 5 月～ http://www.caj.co.jp/etrust/scm	現アンチウイルスソフトだけでは防ぐことができない、スパイウェア、ハッカーツール、キーロガー、DoS といった攻撃／侵入を検知、対応をリアルタイムで実現します。
コンピュータ・アソシエイツ株式会社	eTrust Anti Virus 未定 http://www.caj.co.jp/etrust/antivirus/	サーバ、クライアントPC、グループウェア、ゲートウェイまでウイルスの脅威から保護するアンチウイルスソリューション。2つのウイルススキャニングエンジンでウイルスを完全ブロック。特に企業での利用を前提にして管理機能がすぐれており、運用や導入に大きなメリットとなる。
株式会社インテリジェントウェイブ	ウイルスチェイサー 平成 14 年 7 月～ http://www.viruschaser.jp/	世界的に優れた超高速ウイルス検索エンジン Dr.WEB を使用し、ヒューリスティックスキャン方式を踏まえた独自の方式を採用した強力なシステム監視機能及びメモリ治療機能により二次感染を防止します。又、ディスク容量は約8MBと少なく、完全自動アップデータされる定義ファイルサイズは数KB～数十KBと軽く、常に最新の状態が保たれます。さらに常用化された多くの圧縮ファイルフォーマットに完全対応しています。

開発元	製品名/発売時期/URL	概要・特徴など
株式会社インテリジェントウェイブ	CWAT（Cyber Warning Alert Termination） 平成 15 年 11 月～ http://www.iwi.co.jp/japanese/cwat/news/index.html	CWATはオーガナイゼーションモニタ（統合監視コンソール）、セグメントディフェンスコントローラ（ネットワーク監視）、アンノウンターミナルディフェンスコントローラ（未登録端末監視）、オペレーションディフェンスコントローラ（オペレーション監視）で構成された内部情報漏えい対策システムです。CWATは、ネットワーク情報を監視するだけではなく、外部に持ち出されるモバイルPCやクライアントPCでのFD、CDへの書き出し、外部接続バス経由での未登録端末の直接接続も監視できる機能を持っています。更に、操作員のポリシーに違反した挙動や、普段と著しく異なった挙動を監視することができます。
RSA セキュリティ株式会社	RSA　ClearTrust（アールエスエ・クリアトラスト） 平成 14 年 11 月 1 日頃～ http://www.rsasecurity.co.jp/products/cleartrust/index.html	・認証管理：アクセス管理対象のWebリソースにアクセスするユーザを認証。認証方法としてパスワード、電子証明、ワンタイムパスワード等を使用可能。 ・シングルサインオン：一度認証成功したユーザには、認証トークンを発行。認証トークン有効期間内であれば、ユーザは再度認証することなくWebリソースにアクセス可能。またSAML対応により、異なるネットワークドメインのWebサーバへのシングルサインオンにも対応。 ・ルールに基づくアクセス制御：ユーザID、所属グループ、その他任意のユーザ属性に基づいてのアクセスルールを定義。ルールに合致したユーザのみWebリソースへのアクセスを許可。
RSA セキュリティ株式会社	RSA　Secure ID（アールエスエー・セキュアアイディ） 平成 9 年 1 月 1 日頃～ http://www.rsasecurity.co.jp/products/securid/index.html	一分間隔で変化する乱数を、その時点での時刻と秘匿されている番号から一定のアルゴリズムで成形し表示するカード型のデバイスを、認証を希望する利用者側に配備し、利用者は認証希望時にその時表示されている乱数をパスワードとして認証側に送付する。認証側、例えば一般のアプリケーションは送付されたパスワードを別途設置された認証装置に転送して認証の代行を依頼し、その回答により認証の可否を決定する。認証装置は、パスワード受信時の時刻と予め登録されている当該利用者の秘密番号から利用者デバイスと同じアルゴリズムで乱数を生成し、送付されたパスワードの妥当性（一致）を検証し結果を回答する。
RSA セキュリティ株式会社	RSA　Sign－On　Manager（アールエスエー・サインオンマネージャ）	ユーザ情報やパスワードを記憶するサーバと、ユーザのPC上で動くクライアントで構成されるシングルサインオン技術。ユーザがP

開発元	製品名/発売時期/URL	概要・特徴など
	平成 17 年 10 月 1 日頃～	Cから一旦ICカード等で認証されれば、サーバに事前登録されたWebページやアプリにサインオンする際にIDやパスワードがサーバからダウンロードされる。ユーザがパスワードを記憶する必要が無く複雑なパスワードの設定が可能。ICカード紛失時にユーザが事前登録された個人情報を解答すれば緊急パスワードの発行も可。答えるべき個人情報の数や許容正解率をポリシーで管理でき、ICカードを紛失した場合と忘れた場合等で別々に設定可能。その個人情報はどこにも保存されず、一定の正解率の場合にのみ解答が暗号学的に処理され緊急パスワードが発行される。
	なし	
トップレイヤーネットワークスジャパン株式会社	Attack Mitigator IPS 平成 14 年 3 月～ http://www.TopLayer.co.jp/products/ol_attack.html	Attack Mitigator IPSは、不正アクセスや、悪意のあるコンテンツ(ウイルスやワーム、トロイの木馬その他)及び DoS/DDoS などの量的な攻撃からネットワーク・レベルおよびアプリケーションレベルでの最適なサービスプロテクションを提供する。TipFireTMASICとTopinspectTM詳細パケット分析アルゴリズムによるハイパフォーマンスなアプリケーション使用基準検査により、重要サーバに対する各種のサイバー攻撃を検知および遮断を行い、サーバに脆弱性が内包されている場合も不正侵入を未然に防ぐ。
日立ソフトウェアエンジニアリング株式会社	秘文AE Server 平成 7 年 10 月～ http://hitachisoft.jp/hibun/	秘文はクライアントPCからの情報漏えい防止を行ないます。基本的にはPCにインストールして活用します。そして更にサーバを組み合わせる事により、セキュリティの強度を上げますが、その際にネットワークにつながるPCの各アクセス権限を設定し、これをサーバで管理運用します。
横河電機株式会社	Secure Ticketセキュアチケット 平成 16 年 6 月～ http://www.yokogawa.co.jp/itbiz/secureticket/	SecureTicketはSSL－VPN機能を搭載したWebサーバの総合セキュリティソフトです。 [特徴] ・多様なデバイスをサポートする強力・安全な“ユーザ認証”各種デバイス(USBトークン、USBディスク等)に対応したワンタイムパスワードやバイオメトリスクや、バイオメトリクス、携帯電話に対応しています。 ・多様な認証機能と連携した“SSL－VPN”特別なハード不要！特別なクライアント不要の簡単導入！サービス単位のアクセス制御が可能です。 ・Webサーバへの不正アクセスを強力にブロックする“リバースプロキシ”各種サービスに対するグループ単位のアクセスコントロール、ダイナミックなセッション管理、他認証を統合するシングルサインオンが可能です。
NECネクサソリューションズ株式会社	アプリケーション脆弱性診断サービス 平成 15 年 9 月 1 日頃～	Webアプリケーションのソースを提供いただき、脆弱性を検出するサービス。人的ミスや

開発元	製品名/発売時期/URL	概要・特徴など
	なし	リソースに依存しないように、ソースをスキャンしてオブジェクトレベルに分離する解析補助ツールを開発した。対象はASP、JSP、JavaScriptなどのスクリプト系と、VB、Cttなどの COM系言語にも対応。
NECネクサソリューションズ株式会社	SOLVDEFENCE 未定 http://www.nec-nexs.com/sl/sol/os_msp_solvdefence.html	弊社データセンターとのハウジングユーザー向けセキュリティサービスとして提供されているサーバ防御用ソフトウェア。Windowsサーバ特にWebサーバの防御を目的とする機能は以下の4つ。 ・WebAlerter・・・HTTP構文解析を行ない、不正アクセスを検知遮断。ISAPIフィルタ、ISAPIExtension技術。 ・SystemRecover・・・コンテンツの改ざん検知と即時復旧。 ・LogScan・・・メールサーバとWebサーバのログを解析し、レポートを生成。 ・PermissionCollector・・・IISのアクセス権やオブジェクトを監視。ミスオペレーションを即時通知。
マカフィー株式会社	VirusScanEnterprise8.0i 平成 16 年 8 月 31 日頃～ http://www.mcafee.com/jp	＜VSE＞・ウイルスの他、ワーム、アドウェア/スパイウェア、バッファオーバーフローにも対応。 ・強力なリモート管理。（ひとつのコンソールから、エンタープライズ全体に対し、すべての監視、設定機能が使えます） ・管理者へのアラート機能。（管理者があらゆる組合せのシステムアラートの設定、定義が可能で、それぞれを個別に有効にしたり、優先順位をつけることができます） ・リアルタイムオンデマンドスキャンとスケジュールスキャン対応。 ・ePOとの連携により中央管理とグラフィカルレポートによる統合管理が可能。
株式会社富士通ソーシアルサイエンスラボラトリ	PC/Safeシリーズ 平成 15 年 10 月 15 日頃～ http://www.ssl.fujitsu.com/	PC/Safeシリーズは、富士通のセキュリティソリューション体系の中で、パソコンセキュリティを実施/管理する製品群です。 ・SafeManager・・・パソコンのセキュリティ対策実施状況を一元管理。ウイルス感染対策。ハードウェア、ソフトウェアの資産管理。 ・SafeBoot・・・クラスタレベルでのハードディスクの暗号化、OS起動前のパスワード認証によるパソコンの情報漏えい防止。 ・Safeディスク消去人・・・ハードディスク内容の完全消去により、廃棄したパソコンからの機密データ漏えい防止。 ・SafeDefenseWinPRO・・・パソコン機能制限/環境保護。ファイル/ドライブのアクセス制限。 ・SafeIPWATCHER・・・ネットワーク不正接続や稼動状態監視。機器台帳管理。 ・SafeSecureKeeper・・・サーバの機密制限による情報漏えい防止。 ・SafeSF2000Bio・・・バイオメトリクス認証。

開発元	製品名/発売時期/URL	概要・特徴など
株式会社富士通ソーシアルサイエンスラボラトリ	ShieldWARE 未定 なし	webサーバ、DNS、メールサーバなどのイントラ、インターネット上のサーバを対象とし、サーバ内にあるお客様の大切なデータを保護します。あらかじめ設定されたアクセスルートだけ許可するため、未知、既知や外部、内部を問わず不正な攻撃を OS レベルで遮断します。OS資源へのアクセスを詳細に記録します。また複雑なセキュリティ設定を簡易化し、マルチプラットフォームの複数のサーバを集中管理します。
サン･マイクロシステムズ株式会社	SunScreen Secure Net 未定 http://jp.sun.com/software/security/securenet/	SunScreen Netは、アクセス制御や、認証、ネットデータの暗号化などを行う汎用的な全社向けファイアウォールシステムです。SunScreen Secure Netには、ネットワークのアクセス制御を行うルールベースの動的なパケットフィルタリングエンジンと暗号化/認証エンジンがあります。暗号化/認証エンジンに公開鍵暗号化技術を統合することにより、安全な仮想プライベートネットワーク（VPN）ゲートウェイを作成できます。
サン･マイクロシステムズ株式会社	Trusted Solaris 未定 http://jp.sun.com/software/solaris/trustedsolaris/	高レベルのプライバシー、追跡可能性の向上、セキュリティ違反リスクの軽減を実現し、政府関係機関、情報関係機関、およびセキュリティ関係機関での実績を持ち、金融、健康管理、小売などの業界で足場を固めたTrusted Solaris Operating System（OS）は、商用グレードのOSへのセキュリティの組み込みを実現します。Trusted Solaris OSを使用することによって、デスクトップユーザからデータセンターのユーザまでが、ネットワークのセキュリティリスクを軽減し、セキュリティの信頼性をさらに高めることができます。
サン･マイクロシステムズ株式会社	Solaris 10 未定 http://jp.sun.com/software/solaris/trustedsolaris/	Solaris 10 はエンタープライズを異なったレベルで保護できる。先進的なセキュリティ機能を備えています。このセキュリティシステムは、外部からの悪意を持ったアタックや、内部からの不正なデータアクセスを防ぎます。再設計された暗号化フレームワークは、ハードウェアによる暗号化が可能な場合は自動的にそれを選択することで最適な暗号化メソッドを選択し、柔軟な管理を実現します。Process Rights Managementコンポーネントが、どのユーザをどのプロセスに対し、何時、どのような権限を与えるのか詳細な制御を可能にします。
サン･マイクロシステムズ株式会社	Sun Java System Access Manager 未定	イントラネットとエクストラネットのアクセス制御が可能にする。オープン・スタンダード・ベースのアクセス・マネージャ。Sun Java System Access Managerは、企業の内側からはもとより、B2B（business－to－business）のバリュー・チェーン全体から、企業のWebアプリケーションへのアクセスを可能にするセキュリティ基盤です。オープンなスタ

開発元	製品名/発売時期/URL	概要・特徴など
	http://jp.sun.com/software/identity/access_mgr/	ンダード・ベースの認証機構とポリシーベースの承認を実現する、統合フレームワークを提供します。信頼性の高いネットワークをパートナー/納入先/顧客に提供し、リレーションシップを深めることで増収基盤を構築するだけでなくSSO(シングルサインオン:Single Sign－on)を実現し、現代のニーズとこの先成長していくビジネス・ニーズに応えることが可能で、基本的なアイデンティティ情報とアプリケーション情報をセキュアに提供します。
サン･マイクロシステムズ株式会社	Sun Java System Identity Manager 未定 http://jp.sun.com/software/identity/identity_mgr/	個人情報保護をはじめとして、エンタープライズレベルでの各種情報管理が求められる中、Sun Java System Identity Managerにより、既存のシステムに対するシステム変更を迫ることなく、高い安全性と運用性をもったアイデンティティ・マネジメントを行なうことが可能となります。
サン･マイクロシステムズ株式会社	Sun Crypto Accelerator 未定 http://jp.sun.com/products/networking/sslaccel/	Sun Crypto AcceleratorはEコマース等で標準的に使用されるSSL トランザクション処理を高速化するPCI拡張カードです。Sun Crypto Accelerator1000は、SSL計算処理専用のコプロセッサとして動作し、SSL処理をホストCPUから切り離し(CPUオフロード)ホストCPUの負荷を軽減します。
サン･マイクロシステムズ株式会社	Sun Fire B10p 未定 http://jp.sun.com/products/networking/blades/ssl/	Sun Fire B10p SSLプロキシ・ブレードは、Sun Fireブレードプラットフォームの構成要素として、物理的にも機能的にもシームレスに統合されます。SSLオフローディングのためにカスタムASICとファームウェアで実装されたSun Fire B10p SSLプロキシ・ブレードは、それぞれのサーバのホストCPUによるSSL処理と比較して、最大10倍のSSLトランザクション処理能力を提供します。同時に、ホストCPUのすべてのリソースを、本来のサービス提供に利用できるようになります。
サン･マイクロシステムズ株式会社	Sun N2000 Series Secure Application Switch 未定 http://jp.sun.com/products/networking/n2000/	Sun N2000 Series Secure Application Switchは、効率的なリソース運用/サービス統合/先進のコスト・パフォーマンスで、企業のセキュアなネットワーク・コンピューティング環境構築に伴うコストの複雑性を解消します。Sun N2000 Series Secure Application Switchには、ワイヤ・スピードGigabitアプリケーション・スイッチ/チップ・レベルの組込みセキュリティ／リソースの動的な仮想化技術が統合されています。一つのシステムにこれら技術が統合されているので、既存サーバの負荷分散/SSLの高速化／帯域幅管理などを実現するために、アプライアンスなど独自機能を提供する高価なコンポーネントを必要とせず、大幅なTCO削減や分散型コンピューティング環境の管理を簡素化します。
サイバーソリューション株式会社	CYBER－SPACE 平成 13 年 2 月～ http://www.cybersolution.co.jp	・IDCと監視。 ・ネットワーク(Global, Private), サーバの死活、状態監視と対応(ディスパッチレベル) ・ウイルス対応状況の監視と通知。・情報漏えい監視ツールの販売。

開発元	製品名/発売時期/URL	概要・特徴など
富士通株式会社	Interstage Security Director 平成 12 年 7 月 17 日頃～ http://interstage.fujitsu.com/jp/v6/sd	本製品はインターネット上でサービスを提供する www サーバやアプリケーションサーバのためにセキュリティを確保する製品です。ファイアウォール機能およびアプリケーションゲートウェイ機能（HTTP アプリケーションゲートウェイ機能/OP アプリケーションケートウェイ機能）により不正アクセスの防止、通信データの保護、ユーザ認証、内部サーバの隠蔽等を含む強固なセキュリティソリューションを提供します。携帯端末(I モード）からのアクセスについては、登録された端末のみアクセスを許可することで、セキュリティ強度を高める事も可能です。
富士通株式会社	セキュリティ監視サービス 平成 12 年 9 月 5 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	富士通の SOC：「富士通 IT マネージメントセンタ」より、お客様インターネットサイトを 24 時間 365 日監視し、クラッカーによる不正アクセスに迅速に対応します。また、監視状況を集計・分析して月報（Web 等）を提供します。
富士通株式会社	アタックテストサービス 平成 12 年 9 月 5 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	米国 Qualys Guard, IIS 社の Internet Scanner 等を使用したセキュリティのアセスメントサービス。
富士通株式会社	ファイアウォール運用サービス 平成 15 年 2 月 6 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	お客様の運用に合わせたファイアウォールの最適な設計、構築と 24 時間 365 日監視・障害対応体制の提供により、ファイアウォール運用におけるお客様の負担を大幅に削減する。
富士通株式会社	ウイルス対策サービス 平成 14 年 10 月 21 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	お客様の環境に合わせたウイルス対策システムを構築し、24 時間 365 日ウイルス対策ソフトの稼働監視を実施します。また、エキスパートによるウイルス駆除にも迅速に対応します。
富士通株式会社	Web アプリケーションセキュリティ診断サービス 平成 16 年 6 月 23 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	診断ツールと富士通独自ノウハウで、インフラ・OS・ミドルウェアを診断するサーバスキャンでは対応していない、お客様固有開発の Web アプリケーションの脆弱性を診断・評価・分析し、その危険性と具体的な対策指針をご提供します。
富士通株式会社	エンドポイントセキュリティサービス 平成 16 年 6 月 4 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	システム利用者の運用に Windows セキュリティ修正プログラムの適用やウイルスパターンファイルの更新などのセキュリティ対策をシステムで統合管理する環境をご提供します。
株式会社日立情報システムズ	PKI 認証基盤　SSCom（エスエスコム） 平成 11 年 5 月頃～ http://www.shield.ne.jp/products/sscom/index.html	認証機能とアクセス制御機能を組み合わせた認証基盤ソフトウェア。 特徴： ・Felica、PUPPY、認証トークン、IC カード等の認証媒体を使用し安全な認証を実現。 ・VPN 通信機能により盗聴や改ざんから通信内容を保護。 ・グループアクセス制御による情報アクセス制御。
株式会社日立情報システムズ	ID 管理　SSCom/MDS(Meta-Directory Service) 平成 13 年 5 月頃～	・イントラサーバのログイン情報である uID 及び PW の一元管理と各サーバが持つディレクトリへの反映を自動的に行う。認証基盤のソ

開発元	製品名/発売時期/URL	概要・特徴など
	http://www.shield.ne.jp	フトウェア。 特徴: ・市場にある各種ディレクトリと同期が可能。 ・uID 及び PW の変更等の内容がリアルタイムに各サーバのディレクトリへ反映。 ・既存の uID 及び PW、PKI を適用した認証。

2.3 クライアント(PC)を守る

①「技術の研究開発状況」

クライアントに関する研究開発は、回答数 18 件（全回答者の 65.5%）と最多であったのは、一番影響が大きく、また、経営的にも開発費に見合う利益が得られる可能性があることによるのかもしれない。企業と大学が 9 件づつで企業系の研究開発が多いのは、直接コンシューマに接している企業の必然性があるといえるかもしれない。

研究内容については、さまざまな手法がチャレンジされている。可能性の検討段階から、ビジネスモデル特許を準備しているものまで多岐にわたるが、いろいろな試みを行い、意見交換をして情報共有を行うことも重要であろう。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
株式会社インテック	なし 平成 15 年 4 月～ なし	
リコーテクノシステムズ株式会社	センター型検疫ネットワーク提供サービス 平成 16 年 10 月～ なし	・既要構成をまとめビジネスモデル特許出願準備中。 ・製品の技術検証中。 ・サポート体制模索中。
熊本大学	DNSクエリによるウイルス検知ならびに防御 平成 13 年～ なし	学内のネットワークで実証実験中。
山形大学　工学部	分散ファイアウォールの開発 平成 16 年 4 月 1 日～17 年 3 月 31 日 なし	分散ファイアウォールを実現するための基礎的な検討とプロトタイプの実装を行っている。（具体的な内容は、未発表なので書けない。）
中京大学	MTAによるSpam対策システム 平成 15 年 11 月～ なし	RFC2821を守らないSpamを100%拒否可能。
インテリジェントディスク株式会社	新幹系統 平成 14 年 8 月～17 年 4 月 http://www.intelligentdisc.com/	☆大切な情報（個人情報や重要なデータなど）はハッカーやウイルスの攻撃を受けやすいハードディスクでなく、パソコンのバスラインとは完全に切り離された、自らを自立的かつ能動的に防御可能で、持ち運び容易な電脳盤に保存。いくつも持たされるID、パスワードはユーザに代わって電脳盤が一括管理。さらに電脳盤＋生体認証管理でセキュリティをより強固にし、ユビキタスコンピューティングとセキュリティを同時に実現。☆光ディスクの裏面に配置されたRFiDのicチップが生体情報（指紋、虹彩）を認証し、光ディスク利用者を認定すると同時に、個人の安全（安心）が確保されたネットワークに接続される。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
日立ソフトウェアエンジニアリング株式会社	秘文 Advanced Edition 平成 11 年 1 月～19 年 12 月 http://hitachisoft.Jp/hibun/	
株式会社 NTT ドコモ	小型アンチ・ウイルスエンジン 平成 15 年 10 月～ http://www.nttdocomo.co.jp/new/contents/03/whatnew1017.html	Network Associates, Inc. と共同で携帯電話におけるメール、コンテンツ等のウイルススキャン技術の共同研究を行ってきた。現在、アンチ・ウイルスソフトウェアである「McAfee」のウイルス対策技術をベースにアンチ・ウイルスエンジンの小型化および各携帯電話へのパターンアップデート配信に関する要素技術の開発を行なった。
弘前大学	Intrusion Detection Logic 平成 16 年 4 月～18 年 3 月 なし	論理設計中。
宮崎大学	キーボード入力の監視による不正利用者発見システムの開発 平成 16 年 4 月 1 日～18 年 3 月 31 日 なし	コンピュータ（Windows）の不適切な使用を検知し、不正な操作を抑止することが本システムの目的です。Windows の利用者がキーボード入力を行なっている様子やアプリケーションの起動状況を常に監視し、不適切な文字入力やアプリケーションを起動した際には、その様子をコンピュータの管理者へ自動で連絡し警告を発するシステムです。インターネット上に設置された掲示板などへの不適切な書き込みを行なおうとした際や、違法もしくは違法性の高いソフトの実行を試みる際には、自動でネットワークの切断、コンピュータのシャットダウンを行うことで不適切な使用を抑止し、有害情報へのアクセスやネットワーク犯罪を防止する効果が期待できます。これまでに、Windows 上で入力した文字列や起動したアプリケーションの情報を取得できる監視ソフトのプロトタイプを開発しました。現在は、不適切な操作か否かを判別するアルゴリズムを開発中です。導入先としましては、主に教育機関や一般家庭において子供（未成年）が利用しているコンピュータなどに導入されることを期待しています。企業や自治体での導入におきましては、オペレーションの監視による機密情報の漏洩など、その他の不正な操作の防止に効果を発揮することが期待されます。
サイバーソリューション株式会社	SAMS 平成 15 年 10 月 1 日～16 年 9 月 http://cybersolution.co.jp	Virus発生に関連し、ユーザが対応しているかを監視、検知、警告通知。
奈良先端科学技術大学院大学	ユビキタス環境におけるネットワーク資源提供 平成 15 年 4 月 1 日～17 年 3 月 30 日 なし	ユビキタス環境におけるネットワーク資源提供のための、サービスモデルを提案し、論文を執筆した。現在は、このモデルのプロトタイプシステムを設計、実装している。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
奈良先端科学技術大学院大学	エンドノード主導型　ファイアウォール制御機構 平成 15 年 4 月 1 日～17 年 3 月 31 日 なし	証明書を用いたファイアウォールの動的な制御機構を設計中。通信の可否の判断を端末の情報のみでなく、端末利用者の情報（所属中権限）などで行なえるようにする。
広島大学 情報メディア教育研究センター	脆弱性診断支援ツール 平成 15 年 4 月～ なし	大学等、比較的オープンな環境においては、ネットワークに接続されるサーバやクライアントのセキュリティ脆弱性（OS のパッチ等）の管理が非常に困難である。そのため、組織内の監視センター等からネットワークに接続されたサーバやクライアントに対し、脆弱性診断を行い、問題が発見されたマシンの管理者に対し、警告を出す事になるが、大規模な大学等では、必ずしも効果がない。本システムでは大規模組織の一部を管理する管理者が、脆弱性診断を利用し易くする機能等を提供する。
静岡大学 総合情報処理センター	なし 平成 16 年 4 月～ なし	長時間運用実験を実施中。
株式会社日立情報システムズ	SHIELD/ExLink(シールド/イーエクスリンク) 平成 16 年 10 月～17 年 9 月 今後作成予定	･各種のセキュリティ製品と連携し、セキュリティのインシデントを収集し、（ウイルス・ワーム感染、不正アクセス、情報漏えい、盗聴）セキュリティ運営ポリシーに基づいて、被害の拡大阻止のために各種セキュリティ製品と連携し防御する。（ファイアウォール、接続遮断装置）。 ・システム管理装置との連携。
株式会社日立情報システムズ	SHIELDeXpress i-monitor 平成 16 年 10 月～17 年 9 月 なし	セキュリティ脆弱性及びインシデントの情報を世界及びローカルから収集し、監視対象のサイトに迫る攻撃の脅威を分析する。 ・脅威分析の結果は管理者へ通知。 ・事前に指定された監視対象サイトのセキュリティ運用ポリシーに基づいて、防御処置の自動的な実施。

②「技術の実用化（製品化）状況」

クライアントを守る実用化(製品化)されている技術は、回答数 43 件(全回答者の 39.1%)とサーバ用の製品についで多い。

クライアント(PC)自体に対策を講じるタイプ、暗号化したストレージや通信に関するタイプ、異常トラフィックや通過データ(パケット)などの監視・LOG などを行うタイプ、メールなどのアプリケーションに特化した対策を講じるタイプ、スパイウエアやトロイの木馬系の一般的なアンチウイルスソフトが対応できないものの対策を行うタイプ、デジタル証明書による認証を行うタイプ、バイオメトリクスに関連するタイプ、等々、多彩な種類がある。どれも広義の意味のアクセス制御であり、不正アクセスを防ぐための方策が、狭義の意味のアクセス制御にはとどまっていないことが見て取れる。

開発元	製品名/発売時期/URL	概要・特徴など
ジェイズ・コミュニケーション株式会社	Trustream 平成 16 年 7 月 1 日頃～ http://www.jscom.co.jp/trustream/index.htm	外部より侵入するウイルスから企業LANを守るための包括的高速アンチウイルスゲートウェイサーバであり、フィンランドのエフ・セキュア社からソフト提供を受け開発いたしました。
株式会社東京メトロ	Pointsec 平成 12 年 7 月 1 日頃～ http://www.tokyo.metro.co.jp/security/pointsec/index.html	パソコン内のHDDを丸ごと暗号化するのと、本人認証によるOS起動の「データセキュリティ」と「認証セキュリティ」を融合化したシステム。
リコーテクノシステムズ株式会社	ITSheriff AD・ST・LT 平成 15 年 7 月 4 日頃～ http://www.it-sheriff.jp/	ITSheriff Box(ファイアウォール)による外部攻撃侵入からのネットワーク保護。またウイルス対策を行ないます。監視センターから 24 時間 365 日 ITSheriff Box やお客様サーバ、ネットワーク機器を遠隔監視し、異常検出時の対応を行ないます。さらに月間の監視結果レポート・コンタクトセンターによるお客様対応窓口を提供します。
セキュアコンピューティングジャパン株式会社	Smart Filter 平成 8 年～ http://www.smartfilter.jp	webの適正な利用文化を組織に根付かせることを狙いにした製品であり、62 のカテゴリ別に約 600 万のサイトの情報を格納したデータベースに基づいて業務上、必要であるか否かの判断を下し、アクセス禁止等の処置を行う。近年ではwebアクセスで感染するウイルスの出現や、いわゆるフィッシングなどの多発により業務の効率向上以外にもセキュリティという観点からも注目が高まっている。
シスコシステムズ株式会社	Cisco Security Agent 未定 http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/csa/	CSA はエンドユーザとも呼ばれるサーバおよびクライアントコンピュータに、侵入保護の機能を提供します。
株式会社シマンテック	Symantec Incident Manager 未定 http://www.symantec.com/region/jp/products/sim/	URL を参照。

開発元	製品名/発売時期/URL	概要・特徴など
株式会社シマンテック	Symantec Enterprise Security manager5.5 未定 http://www.symantec.com/region/jp/products/esm/	URL を参照。
株式会社シマンテック	Symantec Event Manager for Antivirus 未定 http://www.symantec.com/region/jp/enterprise/products.html/	URL を参照。
株式会社シマンテック	Symantec Web Security3.0 平成 15 年 9 月～ http://www.symantec.com/region/jp/products/sws/	なし
株式会社シマンテック	Symantec　Client Security2.0 平成 16 年 6 月～ http://www.symantec.com/region/jp/products/scs/	URL を参照。
株式会社シマンテック	Symantec AntiVirus Corporate Edition 平成 16 年 6 月～ http://www.symantec.com/region/jp/enterprise/products.html/	URL を参照下さい。
株式会社シマンテック	Symantec Enterprise Firewall8.0 平成 16 年 6 月～ http://www.symantec.com/region/jp/products/sef/	Symantec Enterprise　firewall は独自のハイブリットアーキテクチャを採用しており、企業ネットワークを様々なネットワーク攻撃力で不正なアクセスから強固に、そしてプロアクティブに保護し、企業の情報資産の活用と保護を促進します。主な機能　・アプリケーションプロキシをそなえたフルインスペクション FW。　・プロキシセキュアド VPN による安全性の高い IPSec　VPN の提供。　・クラスタ構成による冗長化と負荷分散が可能。　・Web ベースの容易な管理。
サン･マイクロシステムズ株式会社	Sun Ray 平成 11 年 9 月 20　日頃～	Sun Ray　Appliance　は、完全にステートレスで管理の必要がないクライアント－ アプライアンスです。そこでは、キーボードなどの入力や画面へのピクセル（画素）の表示のみを行い、すべてのアプリケーションの処理やオペレーティングシステムの動作、データの保存は全てサーバ側で行われます。ユーザは、シンプルな環境のもとで作業を行うことができます。

開発元	製品名/発売時期/URL	概要・特徴など
	http://jp.sun.com/products/desktop/infoappliances/	また、あらゆる資源がサーバ側に集約されているため、システム管理者は集中管理を行うことができます。信頼性やスケーラビリティの高い環境を利用できるのも、Sun Ray Appliance 環境の魅力です。Sun Ray Appliance はデータや状態を一切保持していないステートレスな端末なので、必要な際には簡単に他のアプライアンスと交換をすることができます。 - 豊富なマルチメディア機能 - より低い TCO（Total Cost of Ownership / 総合所有コスト）、より低い管理コスト -Hot Desking によるセッションの可搬性 - 総合面で優れた管理性 - そして「デスクトップマシンのアップグレードは一切不要」
株式会社カオスウェア	VSCAT 平成 16 年 7 月 12 日頃～ http://www.ni.tech.softbank.co.jp/solution/bb-appl/vsc/index.html	（独）情報通信研究機構が米国・日本において、3つの特許権を保持し、(株)カオスウェアが著作権を保持している世界最速のカオス理論を応用したランダムベクトル生成によるストリーム型暗号アルゴリズムであり、当社は本暗号アルゴリズムの安全性評価および論文発表、アプリケーションへの組み込み型ミドルウェアエンジン「VSCAT」、SDKの共同研究開発を行なっています。
沖電気工業株式会社	異常トラフィック監視システム 平成 11 月 9 日頃～ http://www.oki.com/jp/Home/JIS/New/OKI-News/2004/11/z04093.html	異常トラフィック監視システムはトラフィックの状況を監視するプローブ装置と、プローブ装置を管理するマネージャ装置から構成され、最大8台までのプローブ装置を配置することができます。（製品はアプライアンスにて提供）異常トラフィック監視システムには、アプケーション別のトラフィック計測機能、異常トラフィック検出機能、アクション機能があり、ネットワークトラフィックの統計画面から簡易な操作でトラフィック調査が行えるだけでなく、ネットワーク感染型ワームの感染活動を検出することが可能です。本製品は Fast Ethernet 対応のスタンダードモデルと Gigabit Ethernet 対応のハイエンドモデルを揃えました。
セコムトラストネット株式会社	セコム社員証ソリューション（IDONE） 未定 http://www.secomtrust.net/service/s_si/solution.html	入退室管理などのフィジカルセキュリティと、高度な認証技術によるサイバーセキュリティを1枚のICカードで同時に実現するものであり、確実な本人認証により、内部情報漏えい対策にも効果を発揮している。
コンピュータ・アソシエイツ株式会社	eTrust Secure Content Manager 未定	迷惑メール、情報漏えい、e メールに起因する法的責任、ウイルス、悪意あるコンテンツ・プログラム、不快なコンテンツなど、様々な脅威からPCを保護する統合コンテ

開発元	製品名/発売時期/URL	概要・特徴など
	http://www.caj.co.jp/etrust/scm	ンツセキュリティソリューション。ビジネス主導型ポリシーエンジン、機密情報のフィルタリング、警告とアクションの自動化、ポリシーの一元管理、迷惑メールとURLアクセスに関する独自のルール作成など、コンテンツセキュリティに重要な機能を豊富に備えている。
コンピュータ・アソシエイツ株式会社	eTrust Pest Ptrol 平成 17 年 5 月～ http://www.caj.co.jp/etrust/scm	現アンチウイルスソフトだけでは防ぐことができない、スパイウェア、ハッカーツール、キーロガー、DoS といった攻撃／侵入を検知、対応をリアルタイムで実現します。
コンピュータ・アソシエイツ株式会社	eTrust Anti Virus 未定 http://www.caj.co.jp/etrust/antivirus/	サーバ、クライアントPC、グループウェア、ゲートウェイまでウイルスの脅威から保護するアンチウイルスソリューション。2つのウイルススキャニングエンジンでウイルスを完全ブロック。特に企業での利用を前提にして管理機能がすぐれており、運用や導入に大きなメリットとなる。
株式会社インテリジェントウェイブ	ウイルスチェイサー 平成 14 年 7 月～ http://www.viruschaser.jp/	世界的に優れた超高速ウイルス検索エンジン Dr.WEB を使用し、ヒューリスティックスキャン方式を踏まえた独自の方式を採用した強力なシステム監視機能及びメモリ治療機能により二次感染を防止します。又、ディスク容量は約8MBと少なく、完全自動アップデートされる定義ファイルサイズは数KB～数十KBと軽く、常に最新の状態が保たれます。さらに常用化された多くの圧縮ファイルフォーマットに完全対応しています。
株式会社インテリジェントウェイブ	CWAT（Cyber Warning Alert Termination） 平成 15 年 11 月～ http://www.iwi.co.jp/japanese/cwat/news/index.html	CWATはオーガナイゼーションモニタ（統合監視コンソール）、セグメントディフェンスコントローラ（ネットワーク監視）、アンノウンターミナルディフェンスコントローラ（未登録端末監視）、オペレーションディフェンスコントローラ（オペレーション監視）で構成された内部情報漏えい対策システムです。CWATは、ネットワーク情報を監視するだけではなく、外部に持ち出されるモバイルPCやクライアントPCでのFD、CDへの書き出し、外部接続バス経由での未登録端末の直接接続も監視できる機能を持っています。更に、操作員のポリシーに違反した挙動や、普段と著しく異なった挙動を監視することができます。
RSA セキュリティ株式会社	RSA Sign－On Manager（アールエスエー・サインオンマネージャ） 平成 17 年 10 月 1 日頃～	ユーザ情報やパスワードを記憶するサーバと、ユーザのPC上で動くクライアントで構成されるシングルサインオン技術。ユー

開発元	製品名/発売時期/URL	概要・特徴など
	なし	ザがPCから一旦ICカード等で認証されれば、サーバに事前登録されたWebページやアプリにサインオンする際にIDやパスワードがサーバからダウンロードされる。ユーザがパスワードを記憶する必要が無く複雑なパスワードの設定が可能。ICカード紛失時にユーザが事前登録された個人情報を解答すれば緊急パスワードの発行も可。答えるべき個人情報の数や許容正解率をポリシーで管理でき、ICカードを紛失した場合と忘れた場合等で別々に設定可能。その個人情報はどこにも保存されず、一定の正解率の場合にのみ解答が暗号学的に処理され緊急パスワードが発行される。
トップレイヤーネットワークスジャパン株式会社	Secure Controller 平成 16 年 6 月～ http://www.TopLayer.co.jp/products/02_sec.html	Secure Controllerは、ユーザ認証とvZONE機能によるアクセス制御とポリシーベースのQoSを提供。クオリティ株式会社および株式会社PFUが提供するソフトウェアとの組み合わせによりSPCソリューション（PCプロファイル認証および検疫）ネットワークを実現。ブリッジ型の機器であり、既存ネットワークの構成変更は不要である。
日立ソフトウェアエンジニアリング株式会社	秘文AE Server 平成 7 年 10 月～ http://hitachisoft.jp/hibun/	秘文はクライアントPCからの情報漏えい防止を行ないます。基本的にはPCにインストールして活用します。そして更にサーバを組み合わせる事により、セキュリティの強度を上げますが、その際にネットワークにつながるPCの各アクセス権限を設定し、これをサーバで管理運用します。
株式会社 NTT ドコモ	FirstPass 平成 15 年 6 月～ http://www.nttdocomo.co.jp/p_s/firstpass/index.html http://www.nttdocomo.co.jp/p_s/firstpass/outline/index.html	従来のID／パスワード認証に代わる公開鍵暗号基盤（PKI）技術を使ったFOMAの電子認証サービス。ドコモから取得したユーザ証明書を利用することによりFOMAまたはPCとFirstPass対応サイトとの間でSSL相互認証を行う。FirstPassにより、「なりすまし」などのセキュリティ被害に遭いにくくなり、さらに安全で信頼性のあるデータ通信が可能となる。
日立ソフトウェアエンジニアリング株式会社	JP1/秘文 平成 11 年 4 月～ http://www.hitachi-sk.co.jp/products/sewnty/	なし
マカフィー株式会社	VirusScanEnterprise8.0i 平成 16 年 8 月 31 日頃～	＜VSE＞・ウイルスの他、ワーム、アドウェア/スパイウェア、バッファオーバーフロ

開発元	製品名/発売時期/URL	概要・特徴など
	http://www.mcafee.com/jp	一にも対応。 ・強力なリモート管理。(ひとつのコンソールから、エンタープライズ全体に対し、すべての監視、設定機能が使えます) ・管理者へのアラート機能。(管理者があらゆる組合せのシステムアラートの設定、定義が可能で、それぞれを個別に有効にしたり、優先順位をつけることができます) ・リアルタイムオンデマンドスキャンとスケジュールスキャン対応。 ・ePOとの連携により中央管理とグラフィカルレポートによる統合管理が可能。
マカフィー株式会社	VirusScan Asap 平成 13 年 5 月 23 日頃～ http://www.mcafee.com/jp	<ASaP>・プログラム、エンジン、ウイルス定義(DAT)ファイルを完全自動で更新するので手間がなく安心。・(エージェントなので)動作が軽い。エージェント容量はわずか5MB・同LAN内の 1 台がインターネットに接続していれば、全PCの更新が可能。・いつでもどこでもWebでウイルス対策レポート閲覧可能。・100KB程度の差分アップデートにも対応。
株式会社富士通ソーシアルサイエンスラボラトリ	PC/Safeシリーズ 平成 15 年 10 月 15 日頃～ http://www.ssl.fujitsu.com/	PC/Safeシリーズは、富士通のセキュリティソリューション体系の中で、パソコンセキュリティを実施/管理する製品群です。 ・SafeManager・・・パソコンのセキュリティ対策実施状況を一元管理。ウイルス感染対策。ハードウェア、ソフトウェアの資産管理。・SafeBoot・・・クラスタレベルでのハードディスクの暗号化、OS起動前のパスワード認証によるパソコンの情報漏えい防止。 ・Safeディスク消去人・・・ハードディスク内容の完全消去により、廃棄したパソコンからの機密データ漏えい防止。 ・SafeDefenseWinPRO・・・パソコン機能制限/環境保護。ファイル/ドライブのアクセス制限。 ・SafeIPWATCHER・・・ネットワーク不正接続や稼動状態監視。機器台帳管理。 ・SafeSecureKeeper・・・サーバの機密制限による情報漏えい防止。 ・SafeSF2000Bio・・・バイオメトリクス認証。
サン・マイクロシステムズ株式会社.	Sun Ray 平成 11 年 9 月 20 日頃～	Sun Ray Appliance は、完全にステートレスで管理の必要がないクライアント- アプ

開発元	製品名/発売時期/URL	概要・特徴など
	http://jp.sun.com/products/desktop/infoappliances/	ライアンスです。そこでは、キーボードなどの入力や画面へのピクセル（画素）の表示のみを行い、すべてのアプリケーションの処理やオペレーティングシステムの動作、データの保存は全てサーバ側で行われます。ユーザは、シンプルな環境のもとで作業を行うことができます。また、あらゆる資源がサーバ側に集約されているため、システム管理者は集中管理を行うことができます。信頼性やスケーラビリティの高い環境を利用できるのも、Sun Ray Appliance 環境の魅力です。Sun Ray Appliance はデータや状態を一切保持していないステートレスな端末なので、必要な際には簡単に他のアプライアンスと交換をすることができます。 - 豊富なマルチメディア機能 - より低い TCO（Total Cost of Ownership / 総合所有コスト）、より低い管理コスト -Hot Desking によるセッションの可搬性 - 総合面で優れた管理性 - そして「デスクトップマシンのアップグレードは一切不要」
サン・マイクロシステムズ株式会社	SunScreen Secure Net 未定 http://jp.sun.com/software/security/securenet/	SunScreen Netは、アクセス制御や、認証、ネットデータの暗号化などを行う汎用的な全社向けファイアウォールシステムです。SunScreen Secure Netには、ネットワークのアクセス制御を行うルールベースの動的なパケットフィルタリングエンジンと暗号化/認証エンジンがあります。暗号化/認証エンジンに公開鍵暗号化技術を統合することにより、安全な仮想プライベートネットワーク（VPN）ゲートウェイを作成できます。
サン・マイクロシステムズ株式会社	Trusted Solaris 未定 http://jp.sun.com/software/solaris/trustedsolaris/	高レベルのプライバシー、追跡可能性の向上、セキュリティ違反リスクの軽減を実現し、政府関係機関、情報関係機関、およびセキュリティ関係機関での実績を持ち、金融、健康管理、小売などの業界で足場を固めたTrusted Solaris Operating System（OS）は、商用グレードのOSへのセキュリティの組み込みを実現します。Trusted Solaris OSを使用することによって、デスクトップユーザからデータセンターのユーザまでが、ネットワークのセキュリティリスクを軽減し、セキュリティの信頼性をさらに高めることができます。
サン・マイクロシステムズ株式会社	Solaris 10	Solaris 10 はエンタープライズを異なっ

開発元	製品名/発売時期/URL	概要・特徴など
	未定 http://jp.sun.com/software/solaris/trustedsolaris/	たレベルで保護できる。先進的なセキュリティ機能を備えています。このセキュリティシステムは、外部からの悪意を持ったアタックや、内部からの不正なデータアクセスを防ぎます。再設計された暗号化フレームワークは、ハードウェアによる暗号化が可能な場合は自動的にそれを選択することで最適な暗号化メソッドを選択し、柔軟な管理を実現します。Process Rights Managementコンポーネントが、どのユーザをどのプロセスに対し、何時、どのような権限を与えるのか詳細な制御を可能にします。
サイバーソリューション株式会社	CYBER－SPACE 平成 13 年 2 月～ http://www.cybersolution.co.jp	・IDCと監視。 ・ネットワーク(Global, Private), サーバの死活、状態監視と対応(ディスパッチレベル) ・ウイルス対応状況の監視と通知。・情報漏えい監視ツールの販売。
沖電気工業株式会社	アイリスパス 平成 10 年 10 月～ http://www.oki.com/jp/FSC/iris/jp/	アイリスパスは、目のアイリス(虹彩)模様が個人毎に異なることを利用して、個人を認証する装置です。虹彩模様は、生後2年程度で安定し、その後一生変わらないと言われていることと、非常に複雑な模様で形成されていることから、高精度な個人認証が可能です。情報セキュリティ向け認証装置であるアイリスパス-hは、PCとVSBで接続され、PCやネットワークへのログオン時にアイリス認証を行う装置です。入退室管理向け認証装置であるアイリスパス-WGは、重要な施設への入退室をアイリス認証によって管理するシステムです。
NEC システムテクノロジー株式会社	Mobile Protect 平成 16 年 6 月～ http://www.necst.co.jp	・USB メモリを PC の鍵として使う→PC に差し込まれているとき以外は PC がロックされる。 ・USB メモリへファイルを格納すると自動的に暗号化される→USB メモリを差し込んでいる PC では PC のハードディスクも暗号化可能。
富士通株式会社	Interstage Security Director 平成 12 年 7 月 17 日頃～ http://interstage.fujitsu.com/jp/v6/sd	本製品はインターネット上でサービスを提供する www サーバやアプリケーションサーバのためにセキュリティを確保する製品です。ファイアウォール機能およびアプリケーションゲートウェイ機能(HTTP アプリケーションゲートウェイ機能/OP アプリケーションケートウェイ機能)により不正アクセスの防止、通信データの保護、ユーザ認証、内部サーバの隠蔽等を含む強固なセキュリティソリューションを提供します。携帯端末(I モード)からのアクセスについては、登録された端末のみアクセスを許可することで、セキュリティ強度を高める事も可能です。

開発元	製品名/発売時期/URL	概要・特徴など
富士通株式会社	Systemwalker Desktop Encryption 平成 16 年 12 月 27 日頃～ http://systemwalker.fujitsu.com/jo/desktop-encryption/	画期的な暗号化・複合化　利用者は知識不要 ・パソコン内の重要なファイルを暗号化することで、個人情報などを保護します。 ・暗号化対象のフォルダやドライブを設定する事によりその中に保存されるファイルを自動的に暗号化・複合化します。 ・ハードディスク（システムドライブを除く）を丸ごと暗号化することも可能です。 ・外部にファイルを持ち出すためにファイルを暗号化するため、メールや MO などの外部記憶媒体を試用した受け渡しが安全に行えます。 ・暗号化にファイルを圧縮するため、受け渡しするファイルサイズが小さくなり情報量を削減できます。 ・受け渡す相手が Systemwalker Desktop Encryption を導入していない場合は、パスワードつきの自己複合形式ファイルに暗号化して受け渡せます。
富士通株式会社	セキュリティ監視サービス 平成 12 年 9 月 5 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	富士通の SOC:「富士通 IT マネージメントセンタ」より、お客様インターネットサイトを 24 時間 365 日監視し、クラッカーによる不正アクセスに迅速に対応します。また、監視状況を集計・分析して月報（Web 等）を提供します。
富士通株式会社	ファイアウォール運用サービス 平成 15 年 2 月 6 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	お客様の運用に合わせたファイアウォールの最適な設計、構築と 24 時間 365 日監視・障害対応体制の提供により、ファイアウォール運用におけるお客様の負担を大幅に削減する。
富士通株式会社	ウイルス対策サービス 平成 14 年 10 月 21 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	お客様の環境に合わせたウイルス対策システムを構築し、24 時間 365 日ウイルス対策ソフトの稼働監視を実施します。また、エキスパートによるウイルス駆除にも迅速に対応します。
富士通株式会社	エンドポイントセキュリティサービス 平成 16 年 6 月 4 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	システム利用者の運用に Windows セキュリティ修正プログラムの適用やウイルスパターンファイルの更新などのセキュリティ対策をシステムで統合管理する環境をご提供します。
株式会社日立情報システムズ	PKI 認証基盤　SSCom（エスエスコム） 平成 11 年 5 月頃～ http://www.shield.ne.jp/products/sscom/index.html	認証機能とアクセス制御機能を組み合わせた認証基盤ソフトウェア。 特徴: ・Felica、PUPPY、認証トークン、IC カード等の認証媒体を使用し安全な認証を実現。 ・VPN 通信機能により盗聴や改ざんから通信内容を保護。 ・グループアクセス制御による情報アクセス制御。
株式会社日立情報システムズ	認証局　SSCom/CA 平成 13 年 10 月頃～ http://www.shield.ne.jp/	私的デジタル証明書の発行と証明書の管理を行う。 ・発行するデジタル証明書は企業内、庁内等で有効な私的証明書 ・証明書の有効期限は自由に指定 ・証明書紛失時の回復も可能 認証局及び証明書の CPS 作成は別サービス

2.4 通信情報を守る

①「技術の研究開発状況」

通信される情報を守るものは、暗号化、認証、ログ収集・解析などが定番ではあるが、この他に、ユビキタス環境に関するものなども研究されている。また、最近の個人情報保護法やフィッシングに伴った対策製品も準備されているようであるが、人間系の思い込みや油断をついてくるものが多いので、根本的な解決を図るのは難しいかもしれない。技術で対応できる部分と教育や運用で解決すべき部分をきちんと意識して対策を考えなければならないだろう。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
愛媛大学 総合情報メディアセンター	Webサービスの分散認証 平成 16 年 4 月 1 日～17 年 4 月 1 日 なし	2003 年まで学術情報DBをSQL/FTPで運用していたが、Nimda、Slammer等の流行により、インターネット上のDBの分開を止め、Webサービスに置き換えている。(2005年第1半期に完了予定) その後、PGP、X509認証を利用し、Webサービスでも認証と認可の委譲を行うモデルを設計、開発中である。
奈良先端科学技術大学院大学	ユビキタス環境におけるネットワーク資源提供 平成 15 年 4 月 1 日～17 年 3 月 30 日 なし	ユビキタス環境におけるネットワーク資源提供のための、サービスモデルを提案し、論文を執筆した。現在は、このモデルのプロトタイプシステムを設計、実装している。
株式会社日立情報システムズ	SHIELD/ExLink(シールド/イーエクスリンク) 平成 16 年 10 月～17 年 9 月 今後作成予定	･各種のセキュリティ製品と連携し、セキュリティのインシデントを収集し、(ウイルス･ワーム感染、不正アクセス、情報漏えい、盗聴)セキュリティ運営ポリシーに基づいて、被害の拡大阻止のために各種セキュリティ製品と連携し防御する。(ファイアウォール、接続遮断装置)。 ･システム管理装置との連携。
株式会社日立情報システムズ	SHIELDeXpress i-monitor 平成 16 年 10 月～17 年 9 月 なし	セキュリティ脆弱性及びインシデントの情報を世界及びローカルから収集し、監視対象のサイトに迫る攻撃の脅威を分析する。 ･脅威分析の結果は管理者へ通知。 ･事前に指定された監視対象サイトのセキュリティ運用ポリシーに基づいて、防御処置の自動的な実施。
株式会社セキュアブレイン	フィッシング詐欺防御ソリューション(PhishWall) 平成 16 年 10 月 5 日～平成 17 年 3 月 http://www.securebrain.co.jp/	プロトタイプは完了 一月後半のベータ版(評価用)のリリースに向けて開発中

②「技術の実用化（製品化）状況」

実用化されているものは、回答数 27 件（全回答者の 23.6%）であり、数は多くないが、実績のある寿命の長い製品が多いようである。勿論、新しいアイディアや用途を開拓したものも多い。新しいものほど、アプリケーションレイヤに近い部分への対応製品が多いようでもあるが、これもネットワーク層だけではなく、アプリケーションそのものが広く共有して使われるようになってきた現われかもしれない。

開発元	製品名/発売時期/URL	概要・特徴など
日本オラクル株式会社	Oracle Database 10g 平成 15 年 4 月 5 日頃～ http://www.oracle.co.jp	RDBMS 内部に格納された機密性のある情報を保護するための各種機能があります。（一部オプション製品あり）
三菱スペース・ソフトウェア株式会社	MSIESER（エム・シー・サー） 平成 15 年 2 月 14 日頃～ http://www.ryoyo.co.jp/product/system/msieser/index.html	概要：network の通信を記録し、必要なときに解析、復元して network 利用を監視します。また記録されたパケットメンテは暗号化され、原本性を確保し、法的証拠として企業の雇用を守ります。特徴：①優れた安全性（装置のセキュリティ機能）。記録されたデータはハッシュ値が付与され、暗号化されます。管理端末からの操作ログが記録されます。アクセス権限もシステム管理者、データ閲覧者、監査者に細分化されています。②自社は拡張性。記録装置は選択自由で大容量も対応しています。③既存のシステムに一切影響を与えません。スイッチのミラーポートからパケットを取得するためのnetworkへの負荷がかかりません。構成変更も必要ありません。
綜合警備保障株式会社	ALSOK サーバ ID 平成 13 年 9 月 1 日頃～ http://e-shop.alsok.co.jp/corporate/it_sec/	webサーバの正当性の保証。サーバ証明書の発行業務。
シスコシステムズ株式会社	Cisco VPN3000 未定 http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/vpn3000on/	リモートアクセスVPNを実現するプラットフォームです。
株式会社シマンテック	Symantec Gateway Security 300series 平成 16 年 8 月～ http://www.symantec.com/region/jp/products/sgs300/	URL を参照。
株式会社シマンテック	Symantec Gateway Security 5400series 平成 15 年 10 月～ http://www.symantec.com/region/jp/products/sgs/	URL を参照。

開発元	製品名/発売時期/URL	概要・特徴など
株式会社シマンテック	Symantec Enterprise Firewall8.0 平成 16 年 6 月～ http://www.symantec.com/region/jp/products/sef/	Symantec Enterprise firewall は独自のハイブリットアーキテクチャを採用しており、企業ネットワークを様々なネットワーク攻撃力で不正なアクセスから強固に、そしてプロアクティブに保護し、企業の情報資産の活用と保護を促進します。主な機能 ・アプリケーションプロキシをそなえたフルインスペクション FW。 ・プロキシセキュアド VPN による安全性の高い IPSec VPN の提供。 ・クラスタ構成による冗長化と負荷分散が可能。 ・Web ベースの容易な管理。
株式会社カオスウェア	VSCAT 平成 16 年 7 月 12 日頃～ http://www.ni.tech.softbank.co.jp/solution/bb-appl/vsc/index.html	(独)情報通信研究機構が米国・日本において、3つの特許権を保持し、(株)カオスウェアが著作権を保持している世界最速のカオス理論を応用したランダムベクトル生成によるストリーム型暗号アルゴリズムであり、当社は本暗号アルゴリズムの安全性評価および論文発表、アプリケーションへの組み込み型ミドルウェアエンジン「VSCAT」、SDKの共同研究開発を行なっています。
沖電気工業株式会社	e すぷりっと便 平成 16 年 11 月頃～ http://www.oki.com/jp/NBC/netbiz/e_supu.html	「e すぷりっと便」は企業内外を問わず、電子メールや CD-ROM などのメディア形式で受け渡しされている個人情報・機密情報を紛失・盗難から守ります。情報は紛失や盗難が発生した場合、たとえ暗号化されていても情報流失と見なされます。「e すぷりっと便」は大事な情報を秘密分散法(電子割符)により、分割・暗号化し、異なる経路で相手に配送することで安全・確実な情報配送を実現します。
コンピュータ・アソシエイツ株式会社	eTrust Secure Content Manager 未定 http://www.caj.co.jp/etrust/scm	迷惑メール、情報漏えい、e メールに起因する法的責任、ウイルス、悪意あるコンテンツ・プログラム、不快なコンテンツなど、様々な脅威からPCを保護する統合コンテンツセキュリティソリューション。ビジネス主導型ポリシーエンジン、機密情報のフィルタリング、警告とアクションの自動化、ポリシーの一元管理、迷惑メールとURLアクセスに関する独自のルール作成など、コンテンツセキュリティに重要な機能を豊富に備えている。
株式会社 NTT ドコモ	FirstPass 平成 15 年 6 月～ http://www.nttdocomo.co.jp/p_s/firstpass/index.html http://www.nttdocomo.co.jp/p_s/firstpass/outline/index.html	従来のID／パスワード認証に代わる公開鍵暗号基盤(PKI)技術を使ったFOMAの電子認証サービス。ドコモから取得したユーザ証明書を利用することによりFOMAまたはPCとFirst Pass対応サイトとの間でSSL相互認証を行う。FirstPassにより、「なりすまし」などのセキュリティ被害に遭いにくくなり、さらに安全で信頼性のあるデータ通信が可能となる。

開発元	製品名/発売時期/URL	概要・特徴など
サン・マイクロシステムズ株式会社	Sun Ray 平成 11 年 9 月 20 日頃～ http://jp.sun.com/products/desktop/infoappliances/	Sun Ray Appliance は、完全にステートレスで管理の必要がないクライアント- アプライアンスです。そこでは、キーボードなどの入力や画面へのピクセル（画素）の表示のみを行い、すべてのアプリケーションの処理やオペレーティングシステムの動作、データの保存は全てサーバ側で行われます。ユーザは、シンプルな環境のもとで作業を行うことができます。また、あらゆる資源がサーバ側に集約されているため、システム管理者は集中管理を行うことができます。信頼性やスケーラビリティの高い環境を利用できるのも、Sun Ray Appliance 環境の魅力です。Sun Ray Appliance はデータや状態を一切保持していないステートレスな端末なので、必要な際には簡単に他のアプライアンスと交換をすることができます。 - 豊富なマルチメディア機能 - より低い TCO（Total Cost of Ownership / 総合所有コスト）、より低い管理コスト -Hot Desking によるセッションの可搬性 - 総合面で優れた管理性 - そして「デスクトップマシンのアップグレードは一切不要」
サン・マイクロシステムズ株式会社	SunScreen Secure Net 未定 http://jp.sun.com/software/security/securenet/	SunScreen Netは、アクセス制御や、認証、ネットデータの暗号化などを行う汎用的な全社向けファイアウォールシステムです。SunScreen Secure Netには、ネットワークのアクセス制御を行うルールベースの動的なパケットフィルタリングエンジンと暗号化/認証エンジンがあります。暗号化/認証エンジンに公開鍵暗号化技術を統合することにより、安全な仮想プライベートネットワーク（VPN）ゲートウェイを作成できます。
サン・マイクロシステムズ株式会社	Trusted Solaris 未定 http://jp.sun.com/software/solaris/trustedsolaris/	高レベルのプライバシー、追跡可能性の向上、セキュリティ違反リスクの軽減を実現し、政府関係機関、情報関係機関、およびセキュリティ関係機関での実績を持ち、金融、健康管理、小売などの業界で足場を固めたTrusted Solaris Operating System（OS）は、商用グレードのOSへのセキュリティの組み込みを実現します。Trusted Solaris OSを使用することによって、デスクトップユーザからデータセンターのユーザまでが、ネットワークのセキュリティリスクを軽減し、セキュリティの信頼性をさらに高めることができます。
サン・マイクロシステムズ株式会社	Solaris 10 未定 http://jp.sun.com/software/solaris/trustedsolaris/	Solaris 10 はエンタープライズを異なったレベルで保護できる。先進的なセキュリティ機能を備えています。このセキュリティシステムは、外部からの悪意を持ったアタックや、内部からの不正なデータアクセスを防ぎます。再設計された暗号化フレームワークは、ハードウェアによる暗号化が可能な場合は自動的にそれを選択することで最適な暗号化メソッドを選択し、柔軟な管理を実現します。Process Rights Managementコンポーネントが、どのユーザをどのプロセスに対し、何時、どのような権限を与えるのか詳細な制御を可能にします。

開発元	製品名/発売時期/URL	概要・特徴など
サン・マイクロシステムズ株式会社	Sun Java System Access Manager 未定 http://jp.sun.com/software/identity/access_mgr/	イントラネットとエクストラネットのアクセス制御が可能にする。オープン・スタンダード・ベースのアクセス・マネージャ。Sun Java System Access Managerは、企業の内側からもとより、B2B（business－to－business）のバリュー・チェーン全体から、企業のWebアプリケーションへのアクセスを可能にするセキュリティ基盤です。オープンなスタンダード・ベースの認証機構とポリシーベースの承認を実現する、統合フレームワークを提供します。信頼性の高いネットワークをパートナー/納入先/顧客に提供し、リレーションシップを深めることで増収基盤を構築するだけでなくSSO（シングルサインオン：Single Sign－on）を実現し、現代のニーズとこの先成長していくビジネス・ニーズに応えることが可能で、基本的なアイデンティティ情報とアプリケーション情報をセキュアに提供します。
サン・マイクロシステムズ株式会社	Sun Java System Identity Manager 未定 http://jp.sun.com/software/identity/identity_mgr/	個人情報保護をはじめとして、エンタープライズレベルでの各種情報管理が求められる中、Sun Java System Identity Managerにより、既存のシステムに対するシステム変更を迫ることなく、高い安全性と運用性をもったアイデンティティ・マネジメントを行なうことが可能となります。
サン・マイクロシステムズ株式会社	Sun Crypto Accelerator 未定 http://jp.sun.com/products/networking/sslaccel/	Sun Crypto AcceleratorはEコマース等で標準的に使用されるSSL トランザクション処理を高速化するPCI拡張カードです。Sun Crypto Accelerator1000は、SSL計算処理専用のコプロセッサとして動作し、SSL処理をホストCPUから切り離し（CPUオフロード）ホストCPUの負荷を軽減します。
サン・マイクロシステムズ株式会社	Sun Fire B10p 未定 http://jp.sun.com/products/networking/blades/ssl/	Sun Fire B10p SSLプロキシ・ブレードは、Sun Fireブレードプラットフォームの構成要素として、物理的にも機能的にもシームレスに統合されます。SSLオフローディングのためにカスタムASICとファームウェアで実装されたSun Fire B10p SSLプロキシ・ブレードは、それぞれのサーバのホストCPUによるSSL処理と比較して、最大10倍のSSLトランザクション処理能力を提供します。同時に、ホストCPUのすべてのリソースを、本来のサービス提供に利用できるようになります。
サン・マイクロシステムズ株式会社	Sun N2000 Series Secure Application Switch 未定 http://jp.sun.com/products/networking/n2000/	Sun N2000 Series Secure Application Switchは、効率的なリソース運用/サービス統合/先進のコスト・パフォーマンスで、企業のセキュアなネットワーク・コンピューティング環境構築に伴うコストの複雑性を解消します。Sun N2000 Series Secure Application Switchには、ワイヤ・スピードGigabitアプリケーション・スイッチ/チップ・レベルの組込みセキュリティ／リソースの動的な仮想化技術が統合されています。一つのシステムにこれら技術が統合されているので、既存サーバの負荷分散/SSLの高速化／帯域幅管理などを実現するために、アプライアンスなど独自機能を提供する高価なコンポーネントを必要とせず、大幅なTCO削減や分散型コンピューティング環境の管理を簡素化します。

開発元	製品名/発売時期/URL	概要・特徴など
富士通株式会社	Interstage Security Director 平成 12 年 7 月 17 日頃～ http://interstage.fujitsu.com/jp/v6/sd	本製品はインターネット上でサービスを提供する www サーバやアプリケーションサーバのためにセキュリティを確保する製品です。ファイアウォール機能およびアプリケーションゲートウェイ機能（HTTP アプリケーションゲートウェイ機能/OP アプリケーションケートウェイ機能）により不正アクセスの防止、通信データの保護、ユーザ認証、内部サーバの隠蔽等を含む強固なセキュリティソリューションを提供します。携帯端末(I モード）からのアクセスについては、登録された端末のみアクセスを許可することで、セキュリティ強度を高める事も可能です。
富士通株式会社	Systemwalker Desktop Encryption 平成 16 年 12 月 27 日頃～ http://systemwalker.fujitsu.com/jo/desktop-encryption/	画期的な暗号化・複合化　利用者は知識不要 ・パソコン内の重要なファイルを暗号化することで、個人情報などを保護します。 ・暗号化対象のフォルダやドライブを設定する事によりその中に保存されるファイルを自動的に暗号化・複合化します。 ・ハードディスク（システムドライブを除く）を丸ごと暗号化することも可能です。 ・外部にファイルを持ち出すためにファイルを暗号化するため、メールや MO などの外部記憶媒体を試用した受け渡しが安全に行えます。 ・暗号化にファイルを圧縮するため、受け渡しするファイルサイズが小さくなり情報量を削減できます。 ・受け渡す相手が Systemwalker Desktop Encryption を導入していない場合は、パスワードつきの自己複合形式ファイルに暗号化して受け渡せます。
富士通株式会社	Web アプリケーションセキュリティ診断サービス 平成 16 年 6 月 23 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	診断ツールと富士通独自ノウハウで、インフラ･OS･ミドルウェアを診断するサーバスキャンでは対応していない、お客様固有開発の Web アプリケーションの脆弱性を診断・評価・分析し、その危険性と具体的な対策指針をご提供します。
富士通株式会社	エンドポイントセキュリティサービス 平成 16 年 6 月 4 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	システム利用者の運用に Windows セキュリティ修正プログラムの適用やウイルスパターンファイルの更新などのセキュリティ対策をシステムで統合管理する環境をご提供します。
株式会社日立情報システムズ	PKI 認証基盤　SSCom（エスエスコム） 平成 11 年 5 月頃～ http://www.shield.ne.jp/products/sscom/index.html	認証機能とアクセス制御機能を組み合わせた認証基盤ソフトウェア。 特徴： ・Felica、PUPPY、認証トークン、IC カード等の認証媒体を使用し安全な認証を実現。 ・VPN 通信機能により盗聴や改ざんから通信内容を保護。 ・グループアクセス制御による情報アクセス制御。
株式会社日立情報システムズ	認証局　SSCom/CA 平成 13 年 10 月頃～ http://www.shield.ne.jp/	私的デジタル証明書の発行と証明書の管理を行う。 ・発行するデジタル証明書は企業内、庁内等で有効な私的証明書 ・証明書の有効期限は自由に指定 ・証明書紛失時の回復も可能 認証局及び証明書の CPS 作成は別サービス

開発元	製品名/発売時期/URL	概要・特徴など
株式会社日立情報システムズ	ID 管理　SSCom/MDS(Meta-Directory Service) 平成 13 年 5 月頃～ http://www.shield.ne.jp	・イントラサーバのログイン情報である uID 及び PW の一元管理と各サーバが持つディレクトリへの反映を自動的に行う。認証基盤のソフトウェア。 特徴: ・市場にある各種ディレクトリと同期が可能。 ・uID 及び PW の変更等の内容がリアルタイムに各サーバのディレクトリへ反映。 ・既存の uID 及び PW、PKI を適用した認証。

2.5 データを守る

①「技術の研究開発状況」

データを守る研究は、回答数 28 件（全回答者の 34.5%）であった。基礎研究から製品化直前までさまざまな研究が行われているようである。暗号化技術を使っているものや、PKI などかなり複雑な仕様を実現することが求められているが、実際の利用場面としては、最先端の技術の割には地味な存在かもしれない。この分野は今後重要な位置づけを持つと思われるので、更に情報交換を進めなければならないだろう。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
株式会社ハイマックス	エージェント	H16上期にプロトタイプを作成し、一部デモ運用を実施。下期から機能改善pu－2として取込み中。
	平成 16 年 2 月 1 日～17 年 10 月 31 日	
	なし	
京都府立大学	電子透かし	実用化可能レベル。
	平成 15 年 4 月 1 日～16 年 12 月 9 日	
	なし	
デジタルアーツ株式会社	自然　傾向解析技術	・市場調査。 ・プロトタイプの開発、テスト。
	平成 16 年 4 月 1 日～17 年 9 月 30 日	
	なし	
富士通サポートアンドサービス株式会社	バイオ認証プロジェクト	SF2000BTOのバージョンアップ機能を開発中。
	平成 16 年 10 月 1 日～	
	http://www.fes.fujitsu.com/solution/so2fsasproducts/fpolsf2000bto/index.html	
愛媛大学 総合情報メディアセンター	Webサービスの分散認証	2003 年まで学術情報DBをSQL/FTPで運用していたが、Nimda、Slammer等の流行により、インターネット上のDBの分開を止め、Webサービスに置き換えている。（2005年第1半期に完了予定） その後、PGP、X509認証を利用し、Webサービスでも認証と認可の委譲を行うモデルを設計、開発中である。
	平成 16 年 4 月 1 日～17 年 4 月 1 日	
	なし	
日立ソフトウェアエンジニアリング	秘文 Advanced Edition	
	平成 11 年 1 月～19 年 12 月	
	http://hitachisoft.Jp/hibun/	
株式会社 NTT ドコモ	小型アンチ・ウイルスエンジン	Network Associates, Inc. と共同で携帯電話におけるメール、コンテンツ等のウイルススキャン技術の共同研究を行ってきた。現在、アンチ・ウイルスソフトウェアである「McAfee」のウイルス対策技術をベースにアンチ・ウイルスエンジンの小型化および各携帯電話へのパターンアップデート配信に関する要素技術の開発を行なった。
	平成 15 年 10 月～	
	http://www.nttdocomo.co.jp/new/contents/03/whatnew1017.html	

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
NECネクサソリューションズ株式会社	セキュリティ統合型アプライアンスサーバ用ソフトウェアの開発 平成 16 年 12 月 1 日～18 年 2 月 28 日 なし	セキュリティ統合型アプライアンスサーバの研究開発。主な目的は情報漏えいの防止／抑止。保護対象は社内、外を問わず公開されたWebサーバ。HTTP プロトコルに特化したアプリケーションレイヤーフォレンジックシステム。当該アプライアンスサーバはGatewayとして機能し、保護対象のサーバが接続されたネットワークに設置される。 ・データアクセスフォレンジック・・・全てのHTTPログと認証ログを保存、不正アクセスフィルタと連携し、怪しいアクセスログを別途保存。 ・認証フィルタ・・・誰がアクセスしたかを管理する。 ・不正アクセス防御フィルタ・・・SOIVDEFENCEの技術を転用して、不正な挙動を学習する機能強化。 ・リバースプロキシフィルタ・・・Gatewayとして動作させる。
株式会社日立情報システムズ	SHIELD/ExLink(シールド/イーエクスリンク) 平成 16 年 10 月～17 年 9 月 今後作成予定	・各種のセキュリティ製品と連携し、セキュリティのインシデントを収集し、(ウイルス・ワーム感染、不正アクセス、情報漏えい、盗聴)セキュリティ運営ポリシーに基づいて、被害の拡大阻止のために各種セキュリティ製品と連携し防御する。(ファイアウォール、接続遮断装置)。 ・システム管理装置との連携。
株式会社日立情報システムズ	SHIELDeXpress i-monitor 平成 16 年 10 月～17 年 9 月 なし	セキュリティ脆弱性及びインシデントの情報を世界及びローカルから収集し、監視対象のサイトに迫る攻撃の脅威を分析する。 ・脅威分析の結果は管理者へ通知。 ・事前に指定された監視対象サイトのセキュリティ運用ポリシーに基づいて、防御処置の自動的な実施。

②「技術の実用化（製品化）状況」

実用化（製品化）されているデータを守る製品は、回答数 41 件（全回答者の 36.4%）とかなり多い。データの守り方もいろいろな観点から実用化（製品化）されており多彩である。概要・特徴を見ても各社の力の入れ方がわかる。この分野は、個人情報保護法や情報漏えいなどの問題を解決するひとつのポイントになる可能性があるということかもしれない。今後ともいろいろなチャレンジが実用化（製品化）されてくることが予想される。

開発元	製品名/発売時期/URL	概要・特徴など
日本オラクル株式会社	Oracle Database 10g 平成 15 年 4 月 5 日頃～ http://www.oracle.co.jp	RDBMS 内部に格納された機密性のある情報を保護するための各種機能があります。（一部オプション製品あり）
三菱スペース・ソフトウェア株式会社	MSIESER（エム・シー・サー） 平成 15 年 2 月 14 日頃～ http://www.ryoyo.co.jp/product/system/msieser/index.html	概要：network の通信を記録し、必要なときに解析、復元して network 利用を監視します。また記録されたパケットメンテは暗号化され、原本性を確保し、法的証拠として企業の雇用を守ります。特徴：①優れた安全性（装置のセキュリティ機能）。記録されたデータはハッシュ値が付与され、暗号化されます。管理端末からの操作ログが記録されます。アクセス権限もシステム管理者、データ閲覧者、監査者に細分化されています。②自社は拡張性。記録装置は選択自由で大容量も対応しています。③既存のシステムに一切影響を与えません。スイッチのミラーポートからパケットを取得するためのnetworkへの負荷がかかりません。構成変更も必要ありません。
デジタルアーツ株式会社	i-フィルター 平成 10 年 8 月～ http://www.daj.co.jp	インターネットのページをアクセスできるものと、できないものとに分別するwebフィルタリングソフト。また書き込みやファイルアップロードの制限。あるいは書き込んだり書き込もうとした内容を確認することが可能であり、web経由の情報漏えい対策が可能。
ファルシステムコンサルティング株式会社	Wise Point 平成 15 年 4 月 1 日頃～ http://wisepoint.jp/	Wise Pontの主な機能は独自方式の認証。Webアプリケーションに対するシングルサインオン、アクセスコントロール等の機能を持っております。特に認証方式については多種の認証方式（Jパスワード、マトリクスコード、イメージマトリクス、携帯電話ID認証）を持っております。
富士通サポートアンドサービス株式会社	Fsus バイオ認証システム SF2000Bio 平成 10 年9月10日頃～ http://www.fes.fujitsu.com/solution/so2fsasproducts/fpolsf2000bto/index.html	クライアントサーバ型式のシステムで、サーバでの一元管理を複数バイオ、マルチベンダー機能を取り入れたバイオ認証システム。さらに業務システムにタイミングフリーで読み込める API を CXS から取り揃えています。
株式会社メトロ	Pointsec 平成 12 年 7 月 1 日頃～ http://www.tokyo.metro.co.jp/security/pointsec/index.html	パソコン内のHDDを丸ごと暗号化するのと、本人認証によるOS起動の「データセキュリティ」と「認証セキュリティ」を融合化したシステム。

開発元	製品名/発売時期/URL	概要・特徴など
株式会社シマンテック	Symantec Incident Manager 未定 http://www.symantec.com/region/jp/products/sim/	URL を参照。
サン・マイクロシステムズ株式会社	Sun Ray 平成 11 年 9 月 20 日頃～ http://jp.sun.com/products/desktop/infoappliances/	Sun Ray Appliance は、完全にステートレスで管理の必要がないクライアント- アプライアンスです。そこでは、キーボードなどの入力や画面へのピクセル（画素）の表示のみを行い、すべてのアプリケーションの処理やオペレーティングシステムの動作、データの保存は全てサーバ側で行われます。ユーザは、シンプルな環境のもとで作業を行うことができます。また、あらゆる資源がサーバ側に集約されているため、システム管理者は集中管理を行うことができます。信頼性やスケーラビリティの高い環境を利用できるのも、Sun Ray Appliance 環境の魅力です。Sun Ray Appliance はデータや状態を一切保持していないステートレスな端末なので、必要な際には簡単に他のアプライアンスと交換をすることができます。 - 豊富なマルチメディア機能 - より低い TCO（Total Cost of Ownership / 総合所有コスト）、より低い管理コスト -Hot Desking によるセッションの可搬性 - 総合面で優れた管理性 - そして「デスクトップマシンのアップグレードは一切不要」
株式会社カオスウェア	VSCAT 平成 16 年 7 月 12 日頃～ http://www.ni.tech.softbank.co.jp/solution/bb-appl/vsc/index.html	（独）情報通信研究機構が米国・日本において、3つの特許権を保持し、(株)カオスウェアが著作権を保持している世界最速のカオス理論を応用したランダムベクトル生成によるストリーム型暗号アルゴリズムであり、当社は本暗号アルゴリズムの安全性評価および論文発表、アプリケーションへの組み込み型ミドルウェアエンジン「VSCAT」、SDKの共同研究開発を行なっています。
セコムトラストネット株式会社	セコム社員証ソリューション（IDONE） 未定 http://www.secomtrust.net/service/s_si/solution.html	入退室管理などのフィジカルセキュリティと、高度な認証技術によるサイバーセキュリティを1枚のICカードで同時に実現するものであり、確実な本人認証により、内部情報漏えい対策にも効果を発揮している。
セコムトラストネット株式会社	セコム情報金庫 未定 http://www.secomtrust.net/service/s_product/kinko.html	ユーザサイトに設置する小型データセンター。高品質部材のメーカー等を中心に導入が進んでいる。
コンピュータ・アソシエイツ株式会社	eTrust Access Control 未定 http://www.caj.co.jp/etrust/ac	サーバ上のリソース（ファイルやプログラム等）に対するアクセス制御を実現する製品。役割に応じた適切なアクセス権限を設定（適切なユーザに適切な権限を与える）ことが可能。正常アクセスも含む追跡可能な監査ログを取得する。“だれが”、“いつ”、“どの端末から”、“何のツールを使って”、“どのリソースへ”といった4W1Hに基づいたログを出力。ログは誰も改ざんできない仕組みとなっている。

開発元	製品名/発売時期/URL	概要・特徴など
株式会社インテリジェントウェイブ	ウイルスチェイサー 平成 14 年 7 月～ http://www.viruschaser.jp/	世界的に優れた超高速ウイルス検索エンジン Dr.WEB を使用し、ヒューリスティックスキャン方式を踏まえた独自の方式を採用した強力なシステム監視機能及びメモリ治療機能により二次感染を防止します。又、ディスク容量は約8MBと少なく、完全自動アップデートされる定義ファイルサイズは数KB～数十KBと軽く、常に最新の状態が保たれます。さらに常用化された多くの圧縮ファイルフォーマットに完全対応しています。
株式会社インテリジェントウェイブ	CWAT（Cyber Warning Alert Termination） 平成 15 年 11 月～ http://www.iwi.co.jp/japanese/cwat/news/index.html	CWATはオーガナイゼーションモニタ（統合監視コンソール）、セグメントディフェンスコントローラ（ネットワーク監視）、アンノウンターミナルディフェンスコントローラ（未登録端末監視）、オペレーションディフェンスコントローラ（オペレーション監視）で構成された内部情報漏えい対策システムです。CWATは、ネットワーク情報を監視するだけではなく、外部に持ち出されるモバイルPCやクライアントPCでのFD、CDへの書き出し、外部接続バス経由での未登録端末の直接接続も監視できる機能を持っています。更に、操作員のポリシーに違反した挙動や、普段と著しく異なった挙動を監視することができます。
RSA セキュリティ株式会社	RSA　ClearTrust（アールエスエ・クリアトラスト） 平成 14 年 11 月 1 日頃～ http://www.rsasecurity.co.jp/products/cleartrust/index.html	・認証管理：アクセス管理対象のWebリソースにアクセスするユーザを認証。認証方法としてパスワード、電子証明、ワンタイムパスワード等を使用可能。 ・シングルサインオン：一度認証成功したユーザには、認証トークンを発行。認証トークン有効期間内であれば、ユーザは再度認証することなくWebリソースにアクセス可能。またSAML対応により、異なるネットワークドメインのWebサーバへのシングルサインオンにも対応。 ・ルールに基づくアクセス制御：ユーザID、所属グループ、その他任意のユーザ属性に基づいてのアクセスルールを定義。ルールに合致したユーザのみWebリソースへのアクセスを許可。
RSA セキュリティ株式会社	RSA　Secure ID（アールエスエー・セキュアアイディ） 平成 9 年 1 月 1 日頃～ http://www.rsasecurity.co.jp/products/securid/index.html	一分間隔で変化する乱数を、その時点での時刻と秘匿されている番号から一定のアルゴリズムで成形し表示するカード型のデバイスを、認証を希望する利用者側に配備し、利用者は認証希望時にその時表示されている乱数をパスワードとして認証側に送付する。認証側、例えば一般のアプリケーションは送付されたパスワードを別途設置された認証装置に転送して認証の代行を依頼し、その回答により認証の可否を決定する。認証装置は、パスワード受信時の時刻と予め登録されている当該利用者の秘密番号から利用者デバイスと同じアルゴリズムで乱数を生成し、送付されたパスワードの妥当性（一致）を検証し結果を回答する。

開発元	製品名/発売時期/URL	概要・特徴など
RSA セキュリティ株式会社	RSA Sign－On Manager(アールエスエー・サインオンマネージャ) 平成 17 年 10 月 1 日頃～ なし	ユーザ情報やパスワードを記憶するサーバと、ユーザのPC上で動くクライアントで構成されるシングルサインオン技術。ユーザがPCから一旦ICカード等で認証されれば、サーバに事前登録されたWebページやアプリにサインオンする際にIDやパスワードがサーバからダウンロードされる。ユーザがパスワードを記憶する必要が無く複雑なパスワードの設定が可能。ICカード紛失時にユーザが事前登録された個人情報を解答すれば緊急パスワードの発行も可。答えるべき個人情報の数や許容正解率をポリシーで管理でき、ICカードを紛失した場合と忘れた場合等で別々に設定可能。その個人情報はどこにも保存されず、一定の正解率の場合にのみ解答が暗号学的に処理され緊急パスワードが発行される。
日立ソフトウェアエンジニアリング株式会社	秘文AE Server 平成 7 年 10 月～ http://hitachisoft.jp/hibun/	秘文はクライアントPCからの情報漏えい防止を行ないます。基本的にはPCにインストールして活用します。そして更にサーバを組み合わせる事により、セキュリティの強度を上げますが、その際にネットワークにつながるPCの各アクセス権限を設定し、これをサーバで管理運用します。
横河電機株式会社	As－C/h、As－C/m、As－F 平成 15 年 8 月 26 日頃～ http://www.yokogawa.co.jp/itbiz/as/	IEEE802.1XとRADIUS認証ソフトウェアを搭載したアプライアンス製品。IEEE802.1Xは、有線認証スイッチと無線LANに、RADIUSは電話回線(RAS)にクライアントPCを接続する時の認証プロトコルの規定です。これらを搭載するASシリーズは、As－C／h、As－C/m、As－Fの3機種より構成されます。これらは、EAP－TLS、EAP－TTLS、PEAPの認証プロトコルに対応しています。As－C/h、As－C/mでは認証ソフトウェアを加えてCA機能を搭載しデジタル証明書を発行することが可能です。外部のLDAPサーバとの連携も可能です。As－Fは、小型で駆動部がバッテリバックアップ機能を搭載し小規模オフィスや支社支店や各フロアエッジへの配置が可能です。As－Cをセンターに配置し、PROXYよりエッジに配置したAs－Fと分散構成をとることが可能です。
日立ソフトウェアエンジニアリング株式会社	JP1/秘文 平成 11 年 4 月～ http://www.hitachi-sk.co.jp/products/sewnty/	なし

開発元	製品名/発売時期/URL	概要・特徴など
NECネクサソリューションズ株式会社	SOLVDEFENCE 未定 http://www.nec-nexs.com/sl/sol/os_msp_solvdefence.html	弊社データセンターとのハウジングユーザー向けセキュリティサービスとして提供されているサーバ防御用ソフトウェア。Windowsサーバ特にWebサーバの防御を目的とする機能は以下の4つ。 ・WebAlerter・・・HTTP構文解析を行ない、不正アクセスを検知遮断。ISAPIフィルタ、ISAPIExtension技術。 ・SystemRecover・・・コンテンツの改ざん検知と即時復旧。 ・LogScan・・・メールサーバとWebサーバのログを解析し、レポートを生成。 ・PermissionCollector・・・IISのアクセス権やオブジェクトを監視。ミスオペレーションを即時通知。
富士通関西中部ネットテック株式会社	PolicyGuardian 平成 16 年 11 月 1 日頃～ http://www.kcn.fujitsu.com/services/pro_policyG.html	アクセスコントロールを実装する方法として、クライアントやサーバ、ゲートウェイなどに規制機能を持たせることが一般的であるが、本製品は、クライアント利用者に情報セキュリティポリシーを正しく理解させ、自発的なセキュリティ保全行動を促す事を目的として、以下のようなPDSAサイクルで運用されることを特徴とする。 ①情報セキュリティポリシーの策定とリスク許容値の設定（Plan） ②クライアントの日々の運用状態の監視と記録（Do） ③リスク許容値を超える利用者の抽出とポリシー理解度確認テストの実施（Check） ④基準に満たない利用者の再教育、アクセス権制限など（Action） システム構成PolicyGuardianサーバ：RedHatLinux9、クライアント：Windouws 2000/XP IE6.0 SP2 以上
株式会社富士通ソーシアルサイエンスラボラトリ株式会社	PC/Safeシリーズ 平成 15 年 10 月 15 日頃～ http://www.ssl.fujitsu.com/	PC/Safeシリーズは、富士通のセキュリティソリューション体系の中で、パソコンセキュリティを実施/管理する製品群です。 ・SafeManager・・・パソコンのセキュリティ対策実施状況を一元管理。ウイルス感染対策。ハードウェア、ソフトウェアの資産管理。 ・SafeBoot・・・クラスタレベルでのハードディスクの暗号化、OS起動前のパスワード認証によるパソコンの情報漏えい防止。 ・Safeディスク消去人・・・ハードディスク内容の完全消去により、廃棄したパソコンからの機密データ漏えい防止。 ・SafeDefenseWinPRO・・・パソコン機能制限/環境保護。ファイル/ドライブのアクセス制限。 ・SafeIPWATCHER・・・ネットワーク不正接続や稼動状態監視。機器台帳管理。 ・SafeSecureKeeper・・・サーバの機密制限による情報漏えい防止。 ・SafeSF2000Bio・・・バイオメトリクス認証。

開発元	製品名/発売時期/URL	概要・特徴など
株式会社富士通ソーシアルサイエンスラボラトリ株式会社	ShieldWARE 未定 なし	webサーバ、DNS、メールサーバなどのイントラ、インターネット上のサーバを対象とし、サーバ内にあるお客様の大切なデータを保護します。あらかじめ設定されたアクセスルートだけ許可するため、未知、既知や外部、内部を問わず不正な攻撃をOSレベルで遮断します。OS資源へのアクセスを詳細に記録します。また複雑なセキュリティ設定を簡易化し、マルチプラットフォームの複数のサーバを集中管理します。
サン・マイクロシステムズ株式会社	SunScreen Secure Net 未定 http://jp.sun.com/software/security/securenet/	SunScreen Netは、アクセス制御や、認証、ネットデータの暗号化などを行う汎用的な全社向けファイアウォールシステムです。SunScreen Secure Netには、ネットワークのアクセス制御を行うルールベースの動的なパケットフィルタリングエンジンと暗号化/認証エンジンがあります。暗号化/認証エンジンに公開鍵暗号化技術を統合することにより、安全な仮想プライベートネットワーク(VPN)ゲートウェイを作成できます。
サン・マイクロシステムズ株式会社	Trusted Solaris 未定 http://jp.sun.com/software/solaris/trustedsolaris/	高レベルのプライバシー、追跡可能性の向上、セキュリティ違反リスクの軽減を実現し、政府関係機関、情報関係機関、およびセキュリティ関係機関での実績を持ち、金融、健康管理、小売などの業界で足場を固めたTrusted Solaris Operating System(OS)は、商用グレードのOSへのセキュリティの組み込みを実現します。Trusted Solaris OSを使用することによって、デスクトップユーザからデータセンターのユーザまでが、ネットワークのセキュリティリスクを軽減し、セキュリティの信頼性をさらに高めることができます。
サン・マイクロシステムズ株式会社	Solaris 10 未定 http://jp.sun.com/software/solaris/trustedsolaris/	Solaris 10 はエンタープライズを異なったレベルで保護できる。先進的なセキュリティ機能を備えています。このセキュリティシステムは、外部からの悪意を持ったアタックや、内部からの不正なデータアクセスを防ぎます。再設計された暗号化フレームワークは、ハードウェアによる暗号化が可能な場合は自動的にそれを選択することで最適な暗号化メソッドを選択し、柔軟な管理を実現します。Process Rights Managementコンポーネントが、どのユーザをどのプロセスに対し、何時、どのような権限を与えるのか詳細な制御を可能にします。

開発元	製品名/発売時期/URL	概要・特徴など
サン・マイクロシステムズ株式会社	Sun Java System Access Manager 未定 http://jp.sun.com/software/identity/access_mgr/	イントラネットとエクストラネットのアクセス制御が可能にする。オープン・スタンダード・ベースのアクセス・マネージャ。Sun Java System Access Managerは、企業の内側からもとより、B2B（business－to－business）のバリュー・チェーン全体から、企業のWebアプリケーションへのアクセスを可能にするセキュリティ基盤です。オープンなスタンダード・ベースの認証機構とポリシーベースの承認を実現する、統合フレームワークを提供します。信頼性の高いネットワークをパートナー/納入先/顧客に提供し、リレーションシップを深めることで増収基盤を構築するだけでなくSSO（シングルサインオン：Single Sign－on）を実現し、現代のニーズとこの先成長していくビジネス・ニーズに応えることが可能で、基本的なアイデンティティ情報とアプリケーション情報をセキュアに提供します。
サン・マイクロシステムズ株式会社	Sun Java System Identity Manager 未定 http://jp.sun.com/software/identity/identity_mgr/	個人情報保護をはじめとして、エンタープライズレベルでの各種情報管理が求められる中、Sun Java System Identity Managerにより、既存のシステムに対するシステム変更を迫ることなく、高い安全性と運用性をもったアイデンティティ・マネジメントを行なうことが可能となります。
サン・マイクロシステムズ株式会社	Sun Crypto Accelerator 未定 http://jp.sun.com/products/networking/sslaccel/	Sun Crypto AcceleratorはEコマース等で標準的に使用されるSSL トランザクション処理を高速化するPCI拡張カードです。Sun Crypto Accelerator1000は、SSL計算処理専用のコプロセッサとして動作し、SSL処理をホストCPUから切り離し（CPUオフロード）ホストCPUの負荷を軽減します。
サン・マイクロシステムズ株式会社	Sun Fire B10p 未定 http://jp.sun.com/products/networking/blades/ssl/	Sun Fire B10p SSLプロキシ・ブレードは、Sun Fireブレードプラットフォームの構成要素として、物理的にも機能的にもシームレスに統合されます。SSLオフローディングのためにカスタムASICとファームウェアで実装されたSun Fire B10p SSLプロキシ・ブレードは、それぞれのサーバのホストCPUによるSSL処理と比較して、最大10倍のSSLトランザクション処理能力を提供します。同時に、ホストCPUのすべてのリソースを、本来のサービス提供に利用できるようになります。

開発元	製品名/発売時期/URL	概要・特徴など
サン・マイクロシステムズ株式会社	Sun N2000 Series Secure Application Switch 未定 http://jp.sun.com/products/networking/n2000/	Sun N2000 Series Secure Application Switchは、効率的なリソース運用/サービス統合/先進のコスト・パフォーマンスで、企業のセキュアなネットワーク・コンピューティング環境構築に伴うコストの複雑性を解消します。Sun N2000 Series Secure Application Switchには、ワイヤ・スピードGigabitアプリケーション・スイッチ/チップ・レベルの組込みセキュリティ／リソースの動的な仮想化技術が統合されています。一つのシステムにこれら技術が統合されているので、既存サーバの負荷分散/SSLの高速化／帯域幅管理などを実現するために、アプライアンスなど独自機能を提供する高価なコンポーネントを必要とせず、大幅なTCO削減や分散型コンピューティング環境の管理を簡素化します。
富士通株式会社	Interstage Security Director 平成 12 年 7 月 17 日頃～ http://interstage.fujitsu.com/jp/v6/sd	本製品はインターネット上でサービスを提供する www サーバやアプリケーションサーバのためにセキュリティを確保する製品です。ファイアウォール機能およびアプリケーションゲートウェイ機能（HTTP アプリケーションゲートウェイ機能/OP アプリケーションケートウェイ機能）により不正アクセスの防止、通信データの保護、ユーザ認証、内部サーバの隠蔽等を含む強固なセキュリティソリューションを提供します。携帯端末(I モード）からのアクセスについては、登録された端末のみアクセスを許可することで、セキュリティ強度を高める事も可能です。
富士通株式会社	Systemwalker Desktop Encryption 平成 16 年 12 月 27 日頃～ http://systemwalker.fujitsu.com/jo/desktop-encryption/	画期的な暗号化・複合化　利用者は知識不要 ・パソコン内の重要なファイルを暗号化することで、個人情報などを保護します。 ・暗号化対象のフォルダやドライブを設定する事によりその中に保存されるファイルを自動的に暗号化・複合化します。 ・ハードディスク（システムドライブを除く）を丸ごと暗号化することも可能です。 ・外部にファイルを持ち出すためにファイルを暗号化するため、メールや MO などの外部記憶媒体を試用した受け渡しが安全に行えます。 ・暗号化にファイルを圧縮するため、受け渡しするファイルサイズが小さくなり情報量を削減できます。 ・受け渡す相手が Systemwalker Desktop Encryption を導入していない場合は、パスワードつきの自己複合形式ファイルに暗号化して受け渡せます。

開発元	製品名/発売時期/URL	概要・特徴など
富士通株式会社	Secure Package 情報保護サービス 不明 なし	Secure Package 情報保護サービス 情報保護加工(暗号化による配送時のドキュメントの保護) ・配布するドキュメントに対する操作(印刷、保存)を制限できます。 ・ドキュメント参照時に Secure Package センターで認証を行うため、正規の受信者以外はドキュメントを参照できません。 ・送信後のドキュメントを回収(参照不可能)にできます。 ・送信先を誤った場合。 ・交渉打ち切り、社員の退社など参照資格がなくなった場合。 ・ドキュメントの参照行為を確認できます。確認手段には以下の 2 種類があります。 ・履歴情報(送信後画面) ・通知メール
富士通株式会社	Web アプリケーションセキュリティ診断サービス 平成 16 年 6 月 23 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	診断ツールと富士通独自ノウハウで、インフラ・OS・ミドルウェアを診断するサーバスキャンでは対応していない、お客様固有開発の Web アプリケーションの脆弱性を診断・評価・分析し、その危険性と具体的な対策指針をご提供します。
富士通株式会社	エンドポイントセキュリティサービス 平成 16 年 6 月 4 日頃～ http://segroup.fujitsu.com/secure/solution/lineup.html	システム利用者の運用に Windows セキュリティ修正プログラムの適用やウイルスパターンファイルの更新などのセキュリティ対策をシステムで統合管理する環境をご提供します。
富士通株式会社	個人情報休頼対策サービス 平成 16 年 10 月 20 日頃～ http://segroup.fujitsu.com./jp/news/2004/10/20-1.html	個人データの安全管理措置をトータルの支援 ・情報削減の兆候を SOC よりリモート監視。 ・最先端のプロダクト(非接触スマートロード、手のひら静脈認証、操作抑止ツール、暗号化ツール、入退室管理等)を含めた PDCA 一貫したソルーション。
株式会社日立情報システムズ	PKI 認証基盤 SSCom(エスエスコム) 平成 11 年 5 月頃～ http://www.shield.ne.jp/products/sscom/index.html	認証機能とアクセス制御機能を組み合わせた認証基盤ソフトウェア。 特徴: ・Felica、PUPPY、認証トークン、IC カード等の認証媒体を使用し安全な認証を実現。 ・VPN 通信機能により盗聴や改ざんから通信内容を保護。 ・グループアクセス制御による情報アクセス制御。
株式会社日立情報システムズ	認証局 SSCom/CA 平成 13 年 10 月頃～ http://www.shield.ne.jp/	私的デジタル証明書の発行と証明書の管理を行う。 ・発行するデジタル証明書は企業内、庁内等で有効な私的証明書 ・証明書の有効期限は自由に指定 ・証明書紛失時の回復も可能 認証局及び証明書の CPS 作成は別サービス

開発元	製品名/発売時期/URL	概要・特徴など
株式会社日立情報システムズ	ID 管理　SSCom/MDS(Meta-Directory Service) 平成 13 年 5 月頃～ http://www.shield.ne.jp	・イントラサーバのログイン情報である uID 及び PW の一元管理と各サーバが持つディレクトリへの反映を自動的に行う。認証基盤のソフトウェア。 特徴: ・市場にある各種ディレクトリと同期が可能。 ・uID 及び PW の変更等の内容がリアルタイムに各サーバのディレクトリへ反映。 ・既存の uID 及び PW、PKI を適用した認証。

2.6 施設を守る

①「技術の研究開発状況」

施設を守る IT 技術というと、バイオメトリクス系のものが多いようだが、単純な技術だけではなく、既存の警備システムなどとも複合化されたものが研究されているようである。その意味で、IT 技術セキュリティと物理セキュリティの境界を含み、新しい技術と既存の知恵が相補しあう場面のひとつであろう。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
綜合警備保障株式会社	出入管理システム	システムの実現可能性について調査検討を行なっている。
	平成 15 年 1 月 1 日～17 年 3 月 31 日	
	なし	

②「技術の実用化（製品化）状況」

回答数は 5 件（全回答者の 5.5%）と今回のアンケートの選択肢では一番少なかったが、買ってきて直ぐ使えるものではないことを考えると、地味ではあるが、今後 ISMS などの認証を取る際などに必要な部分であると認識されているようである。特に内部情報漏えい関係で注目度は高いのかもしれない。電子的な部分と物理的な部分のアクセス制御の接点という意味で、今後必要となる技術なのであろう。

開発元	製品名/発売時期/URL	概要・特徴など
株式会社タイテック	なし	施設出入口の開施錠権限者を認証する。
	未定	
	なし	
セコムトラストネット株式会社	セコム社員証ソリューション（IDONE）	入退室管理などのフィジカルセキュリティと、高度な認証技術によるサイバーセキュリティを1枚のICカードで同時に実現するものであり、確実な本人認証により、内部情報漏えい対策にも効果を発揮している。
	未定	
	http://www.secomtrust.net/service/s_si/solution.html	
セコムトラストネット株式会社	セコム情報金庫	ユーザサイトに設置する小型データセンター。高品質部材のメーカー等を中心に導入が進んでいる。
	未定	
	http://www.secomtrust.net/service/s_product/kinko.html	
株式会社インテリジェントウェイブ	CWAT（Cyber Warning Alert Termination）	CWATはオーガナイゼーションモニタ（統合監視コンソール）、セグメントディフェン
	平成 15 年 11 月～	

開発元	製品名/発売時期/URL	概要・特徴など
	http://www.iwi.co.jp/japanese/cwat/news/index.html	スコントローラ(ネットワーク監視)、アンノウンターミナルディフェンスコントローラ(未登録端末監視)、オペレーションディフェンスコントローラ(オペレーション監視)で構成された内部情報漏えい対策システムです。CWATは、ネットワーク情報を監視するだけではなく、外部に持ち出されるモバイルPCやクライアントPCでのFD、CDへの書き出し、外部接続バス経由での未登録端末の直接接続も監視できる機能を持っています。更に、操作員のポリシーに違反した挙動や、普段と著しく異なった挙動を監視することができます。
沖電気工業株式会社	アイリスパス 平成 10 年 10 月～ http://www.oki.com/jp/FSC/iris/jp/	アイリスパスは、目のアイリス(虹彩)模様が個人毎に異なることを利用して、個人を認証する装置です。虹彩模様は、生後2年程度で安定し、その後一生変わらないと言われていることと、非常に複雑な模様で形成されていることから、高精度な個人認証が可能です。情報セキュリティ向け認証装置であるアイリスパス-hは、PCとVSBで接続され、PCやネットワークへのログオン時にアイリス認証を行う装置です。入退室管理向け認証装置であるアイリスパス-WGは、重要な施設への入退室をアイリス認証によって管理するシステムです。

2.7 その他

①「技術の研究開発状況」

その他としては、Web サービスでの分散認証や、個人情報漏えいに関するフィッシング対策などが、最近の傾向としてあげられる。今回の調査では、現状のインターネット環境を前提にしたものに対する回答があったが、新しい国際標準を作っていくことが必要な時期になっているようにも思われる。

企業大学名	研究開発名称/研究開発期間/URL	技術開発状況
愛媛大学 総合情報メディアセンター	Webサービスの分散認証 平成 16 年 4 月 1 日～17 年 4 月 1 日 なし	2003 年まで学術情報DBをSQL/FTPで運用していたが、Nimda、Slammer等の流行により、インターネット上のDBの分開を止め、Webサービスに置き換えている。(2005年第1半期に完了予定) その後、PGP、X509認証を利用し、Webサービスでも認証と認可の委譲を行うモデルを設計、開発中である。
株式会社セキュアブレイン	フィッシング詐欺防御ソリューション(PhishWall) 平成 16 年 10 月 5 日～平成 17 年 3 月 http://www.securebrain.co.jp/	プロトタイプは完了 一月後半のベータ版(評価用)のリリースに向けて開発中

②「技術の実用化（製品化）状況」

Web フィルターや、伝送経路の工夫、シングルサイオンオン、ID/パスワードの一元管理、正しいアクセスパターンのみ通過させる、など、広い意味でのアクセス制御ではあるが、アプリケーションよりの複合製品が多い。これ等は、必要に応じて選択されるものだろう。今後このような複合製品は増えてくると思われる。

開発元	製品名/発売時期/URL	概要・特徴など
デジタルアーツ株式会社	i-フィルター 平成 10 年 8 月～ http://www.daj.co.jp	インターネットのページをアクセスできるものと、できないものとに分別するwebフィルタリングソフト。また書き込みやファイルアップロードの制限。あるいは書き込んだり書き込もうとした内容を確認することが可能であり、web経由の情報漏えい対策が可能。
セキュアコンピューティングジャパン株式会社	Smart Filter 平成 8 年～ http://www.smartfilter.jp	webの適正な利用文化を組織に根付かせることを狙いにした製品であり、62 のカテゴリ別に約 600 万のサイトの情報を格納したデータベースに基づいて業務上、必要であるか否かの判断を下し、アクセス禁止等の処置を行う。近年ではwebアクセスで感染するウイルスの出現や、いわゆるフィッシングなどの多発により業務の効率向上以外にもセキュリティという観点からも注目が高まっている。

開発元	製品名/発売時期/URL	概要・特徴など
沖電気工業株式会社	e すぷりっと便 平成 16 年 11 月頃～ http://www.oki.com/jp/NBC/netbiz/e_supu.html	「e すぷりっと便」は企業内外を問わず、電子メールや CD-ROM などのメディア形式で受け渡しされている個人情報・機密情報を紛失・盗難から守ります。情報は紛失や盗難が発生した場合、たとえ暗号化されていても情報流失と見なされます。「e すぷりっと便」は大事な情報を秘密分散法（電子割符）により、分割・暗号化し、異なる経路で相手に配送することで安全・確実な情報配送を実現します。
コンピュータ・アソシエイツ株式会社	eTrust Security Command Center 平成 17 年 3 月～ http://www.caj.co.jp/	企業内の様々なOS、セキュリティ製品から発生する情報を一元管理し、複数のイベントより問題の根源となるセキュリティインシデントを分析、また企業レベルでのリスク診断に役立てることができる。セキュリティ情報管理を実現する。セキュリティ業務にかかる現在のコストを削減しながら、様々なリスクに晒される可能性を最小限に低減できるようになる。
RSA セキュリティ株式会社	RSA Sign－On Manager（アールエスエー・サインオンマネージャ） 平成 17 年 10 月 1 日頃～ なし	ユーザ情報やパスワードを記憶するサーバと、ユーザのPC上で動くクライアントで構成されるシングルサインオン技術。ユーザがPCから一旦ICカード等で認証されれば、サーバに事前登録されたWebページやアプリにサインオンする際にIDやパスワードがサーバからダウンロードされる。ユーザがパスワードを記憶する必要が無く複雑なパスワードの設定が可能。ICカード紛失時にユーザが事前登録された個人情報を解答すれば緊急パスワードの発行も可。答えるべき個人情報の数や許容正解率をポリシーで管理でき、ICカードを紛失した場合と忘れた場合等で別々に設定可能。その個人情報はどこにも保存されず、一定の正解率の場合にのみ解答が暗号学的に処理され緊急パスワードが発行される。
株式会社富士通ソーシアルサイエンスラボラトリ	TEROS 平成 16 年 11 月 3 日頃～ http://www.teros.com	Webアプリの脆弱性を回避できる。Webアプリは購入品もあるため、単に修正とはいかないため、問題点を知り、正しいパスのみの通過としている。
株式会社日立情報システムズ	ID 管理 SSCom/MDS(Meta-Directory Service) 平成 13 年 5 月頃～ http://www.shield.ne.jp	・イントラサーバのログイン情報である uID 及び PW の一元管理と各サーバが持つディレクトリへの反映を自動的に行う。認証基盤のソフトウェア。 特徴： ・市場にある各種ディレクトリと同期が可能。 ・uID 及び PW の変更等の内容がリアルタイムに各サーバのディレクトリへ反映。 ・既存の uID 及び PW、PKI を適用した認証。

付属資料

付属資料

1. 調査票

1.1『連絡先記入用紙』

公開情報及びご連絡先記入用紙

※本用紙は調査票と共にご返送お願いいたします。

１．ご回答頂いた技術開発状況を「個別事例一覧表」として本調査の報告書に記載いたします際に下記の情報を公開いたします。公開して差し支えのない範囲で下記項目にご記入ください。

【公開情報用情報】

貴事業体名	
代表者名	
所在地	〒　　－
窓口部署名	
電話番号	
ホームページの URL	

２．本調査に関しまして、特定非営利活動法人日本ネットワークセキュリティ協会がお話をお伺いさせていただいてもよろしければ、差し支えのない範囲で、下記にお名前とご連絡先をご記入ください。

【ご回答者のご連絡先】

貴社名	
貴部署名	
ご担当者氏名	
ご住所	〒
電話番号	
e-mail	

ご連絡先をご記入いただいた方には、別途、特定非営利活動法人日本ネットワークセキュリティ協会からご連絡させていただくことがあります。

【個人情報のお取り扱いについて】

- ■ ご回答者の個人情報は、特定非営利活動法人日本ネットワークセキュリティ協会が適切な保護措置を講じ、厳重に管理いたします。
- ■ ご回答者の回答内容とご連絡先は、不正アクセス行為対策等の実態の把握・今後の方向性の検討等の実施、及び回答内容のご確認のため以外には利用いたしません。また、ご回答内容からご回答者の個人情報が特定される形で調査結果が公開されることはありません。
- ■ 本調査結果の集計・分析作業の一部は株式会社三菱総合研究所に委託予定のため、別紙調査票のご回答内容のみ同社に提供することがありますが、本アンケートで収集したご回答者名・連絡先等の個人情報を、同社を含む外部事業者に提供・預託する予定はありません。
- ■ 当該業務終了後は、特定非営利活動法人日本ネットワークセキュリティ協会が責任を持って個人情報を破棄いたします。

1.2『回答用紙 A』

アクセス制御機能に関する技術の研究開発状況の調査

■ 研究開発の分野については最後のページ「表 1 アクセス制御機能の分類表」を参考にしてください。
■ 研究開発が海外ベンダーで行われている場合は、回答できる範囲でお答えください。

問 1. 現在、取り組んでいるのはどのような分野ですか。(○はいくつでも)

1. 暗号技術
2. 認証技術
3. ネットワークセキュリティ
4. 不正侵入対策
5. セキュリティマネジメント
6. ウイルス対策
7. セキュリティサービス関連
8. その他(　　)
9. 技術開発に取り組んでいない

問 2. 今後、取り組む予定がある分野はどちらですか。(○はいくつでも)

1. 暗号技術
2. 認証技術
3. ネットワークセキュリティ
4. 不正侵入対策
5. セキュリティマネジメント
6. ウイルス対策
7. セキュリティサービス関連
8. その他(　　)
9. 特に計画は無い

問 3. 問 2 で回答いただいた中で、今後もっとも力を入れていく分野はどちらですか。(○は 1 つ)

1. 暗号技術
2. 認証技術
3. ネットワークセキュリティ
4. 不正侵入対策
5. セキュリティマネジメント
6. ウイルス対策
7. セキュリティサービス関連
8. その他(　　)
9. 特に無い

問 4. 現在、実用化(製品化)されている分野をお答えください。(○はいくつでも)

1. 暗号技術
2. 認証技術
3. ネットワークセキュリティ
4. 不正侵入対策
5. セキュリティマネジメント
6. ウイルス対策
7. セキュリティサービス関連
8. その他(　　)
9. 実用化(製品化)されているものは無い

問 5. 今後、実用化(製品化)を見込んでいる分野をご回答ください。(○はいくつでも)

1. 暗号技術
2. 認証技術
3. ネットワークセキュリティ
4. 不正侵入対策
5. セキュリティマネジメント
6. ウイルス対策
7. セキュリティサービス関連
8. その他(　　)
9. 実用化(製品化)の予定は無い

問 6. 貴事業体のおおよその年間売上と、おおよそのアクセス制御関連の年間売上をご回答ください。（単位に注意）

年間売上全体　　およそ＿＿＿＿＿＿万円
その内、アクセス制御関連の年間売上　　およそ＿＿＿＿＿＿万円

問 7. 貴事業体のおおよその年間の研究開発費をご回答ください。（単位に注意）

年間研究開発費　　およそ＿＿＿＿＿＿万円

問 8. 貴事業体で研究開発に携わっているおおよその人員数をご回答ください。

研究開発人員　　およそ＿＿＿＿＿＿人

1.3『回答用紙 B』

実用化(製品化)されているアクセス制御機能に関する技術の個別調査

■ 1 製品(ハードウェア、ソフトウェア、サービス)につき 1 枚の回答用紙をご使用ください。
■ 対象がハードウェアやソフトウェアの場合は、問4は回答いただかなくて結構です。
■ 対象がサービスの場合は、問1～問3は回答いただかなくて結構です。
■ 製品が複数ある場合は、この用紙をコピーしてご記入ください。
■ (※)の付いた用語については最後のページの「表 2 用語説明」を参考にしてください。

製品名	
開発元(メーカー名等)	
開発国	
問1. 何を守りますか (○はいくつでも)	1. ネットワーク　2. サーバ　3. クライアント(PC 等)　4. 通信情報(※) 5. データ　6. 施設(※)　7. その他(　　)
問2. 何から保護しますか (○はいくつでも)	1. 盗聴　2. 漏えい　3. 改ざん(※)　4. なりすまし(※)　5. 事実否認(※) 6. 侵入　7. 踏み台(※)　8. DoS(※)　9. ウイルス 10. その他(　　)
問3. どのような機能を持っていますか (○はいくつでも)	1. 認証(※)　2. 証明書　3. 認可(※)　4. アクセス制御　5. 暗号 6. 検知　7. 運用管理　8. 評価(※) 9. 対外部者の監視　10. 対内部者の監視　11 解析 12. その他(　　)
問4. どのようなサービスですか(対象がサービスの場合) (○はいくつでも)	1. 教育　2. アウトソース　3. インテグレーション　4. コンサルティング 5. 保守(サポート)　6. サービスプロバイダ　7. 保険 8. その他(　　)
概要・特徴など	
価格	
発売時期	平成　　年　　月　　日頃～
出荷本数	累計
製品説明がされている URL	http://

1.4『回答用紙 C』

研究開発中のアクセス制御機能に関する技術の個別調査

■ 1 研究開発分野(技術、サービス)につき 1 枚の回答用紙を使用ください。
■ 研究開発対象が技術の場合は、問4は回答いただかなくて結構です。
■ 研究開発対象がサービスの場合は、問1～問3は回答いただかなくて結構です。
■ 研究開発中の技術・サービスが複数ある場合は、この用紙をコピーしてご記入ください。
■ (※)の付いた用語については最後のページの「表 2 用語説明」を参考にしてください。

関連部門名	
研究開発名称	
研究開発国	
問1．何を守りますか（○はいくつでも）	1．ネットワーク　2．サーバ　3．クライアント(PC 等)　4．通信情報(※) 5．データ　6．施設(※)　7．その他(　　)
問2．何から保護しますか（○はいくつでも）	1．盗聴　2．漏えい　3．改ざん(※)　4．なりすまし(※)　5．事実否認(※) 6．侵入　7．踏み台(※)　8．DoS(※)　9．ウイルス 10．その他(　　)
問3．どのような機能を持っていますか（○はいくつでも）	1．認証(※)　2．証明書　3．認可(※)　4．アクセス制御　5．暗号 6．検知　7．運用管理　8．評価(※) 9．対外部者の監視　10．対内部者の監視　11．解析 12．その他(　　)
問4．どのようなサービスですか（サービスの場合）（○はいくつでも）	1．教育　2．アウトソース　3．インテグレーション　4．コンサルティング 5．保守(サポート)　6．サービスプロバイダ　7．保険 8．その他(　　)
研究開発状況	
研究開発期間	平成　　年　　月　　日～平成　　年　　月　　日
商品説明がされている URL	http://

＜回答用紙 A の補足＞

表 1 アクセス制御機能の分類表

分類	例
暗号技術	暗号技術（アルゴリズム開発など）、暗号化ソフト（ファイルの暗号化、ディスクの暗号化など）
認証技術	ワンタイムパスワード、IC カード、USB 等デバイスによる認証、バイオメトリクス認証、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	VPN（IPsec、SSL、Secure Shell など）、無線 LAN セキュリティ、ファイアウォール、パケットフィルタリング、コンテンツセキュリティ（コンテンツフィルタ、メールフィルタ）、ネットワーク管理
不正侵入対策	侵入検知（IDS）、ハニーポット、アクセスログ収集管理
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（不正プログラム）対策	ウイルス対策ソフト、スパイウェア対策ソフト
セキュリティサービス	セキュリティ診断、不正アクセスウイルス監視、コンサルティング、レスキューサービス

＜回答用紙 B･C の補足＞

表 2 用語の説明

用　語	説　明
通信情報	ネットワークなど通信経路上を流れている情報です。
施設	建屋や部屋を指しますが、広義に電源設備などを含めても結構です。
改ざん	保存されている情報やネットワークなどを流れている情報が、第三者により書き換えられることを意味します。
なりすまし	他人のふりをしてメールを交換したり、情報や金銭を引き出したりする行為です。IP アドレスのなりすまし等も含みます。
事実否認	事実を認めないことを意味します。例えば、発注をしていながら、後にそのようなことが無かったかのように振舞うことです。
踏み台	攻撃者が他人のコンピュータなどを経由することで身元を隠匿するような場合、経由されたコンピュータを踏み台と呼びます。
DoS	インターネット上で、特定のサーバやサイトに向けて一斉に大量の通信を試みることで、当該サーバやサイトのサービスを妨害する攻撃手法です。
認証	パスワードや電子署名、バイオメトリクス認証により、人物（又はシステム）の正当性を確認する行為。
認可	認証後の、細かなサービス･ファイル等の利用許可･制限等やサーバへのアクセス許可･制限等
評価	一定の基準に沿って機能や性能を検証することです。例えば、脆弱性調査ツールなど。

2. 集計表

2.1 回答用紙 A の集計表

		全体	Q1 取り組み分野								
			暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	セキュリティサービス関連	その他	技術開発に取り組んでいない
合計		101	28	41	44	32	34	26	33	12	31
		100.0	27.7	40.6	43.6	31.7	33.7	25.7	32.7	11.9	30.7
F属性	企業	50	14	26	25	20	23	14	26	7	10
		100.0	28.0	52.0	50.0	40.0	46.0	28.0	52.0	14.0	20.0
	大学	44	12	13	14	10	8	10	4	5	19
		100.0	27.3	29.5	31.8	22.7	18.2	22.7	9.1	11.4	43.2

		全体	Q2 取り組み予定分野								
			暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	セキュリティサービス関連	その他	特に計画は無い
合計		101	23	29	34	21	31	14	27	11	35
		100.0	22.8	28.7	33.7	20.8	30.7	13.9	26.7	10.9	34.7
F属性	企業	50	13	20	19	14	21	9	20	7	12
		100.0	26.0	40.0	38.0	28.0	42.0	18.0	40.0	14.0	24.0
	大学	44	9	8	12	6	8	4	5	4	20
		100.0	20.5	18.2	27.3	13.6	18.2	9.1	11.4	9.1	45.5

		全体	Q3 今後もっとも力を入れていく分野								
			暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	セキュリティサービス関連	その他	特に無い
合計		101	5	10	8	1	12	0	9	5	35
		100.0	5.0	9.9	7.9	1.0	11.9	0.0	8.9	5.0	34.7
F属性	企業	50	1	7	3	1	5	0	7	2	12
		100.0	2.0	14.0	6.0	2.0	10.0	0.0	14.0	4.0	24.0
	大学	44	4	3	3	0	5	0	2	3	20
		100.0	9.1	6.8	6.8	0.0	11.4	0.0	4.5	6.8	45.5

		全体	Q4 実用化分野								
			暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	セキュリティサービス関連	その他	実用化されているものは無い
合計		101	16	21	22	14	19	13	21	5	41
		100.0	15.8	20.8	21.8	13.9	18.8	12.9	20.8	5.0	40.6
F属性	企業	50	12	19	18	11	16	10	18	4	12
		100.0	24.0	38.0	36.0	22.0	32.0	20.0	36.0	8.0	24.0
	大学	44	2	0	1	1	0	1	0	1	26
		100.0	4.5	0.0	2.3	2.3	0.0	2.3	0.0	2.3	59.1

		全体	Q5 今後実用化分野								
			暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	セキュリティサービス関連	その他	実用化予定は無い
合計		101	8	19	16	8	17	5	16	8	37
		100.0	7.9	18.8	15.8	7.9	16.8	5.0	15.8	7.9	36.6
F属性	企業	50	8	16	13	7	13	5	13	5	13
		100.0	16.0	32.0	26.0	14.0	26.0	10.0	26.0	10.0	26.0
	大学	44	0	3	2	1	2	0	2	3	21
		100.0	0.0	6.8	4.5	2.3	4.5	0.0	4.5	6.8	47.7

		全体	Q6① 年間売上全体					
			なし	～10億円未満	10億～100億円未満	100億～1,000億円未満	1,000億円以上	不明
合計		101	5	9	9	12	8	58
		100.0	5.0	8.9	8.9	11.9	7.9	57.4
F属性	企業	50	1	7	8	11	7	16
		100.0	2.0	14.0	16.0	22.0	14.0	32.0
	大学	44	4	1	0	0	0	39
		100.0	9.1	2.3	0.0	0.0	0.0	88.6

		全体	Q6② その内、アクセス制御関連の年間売上				
			なし	～1億円未満	1億～10億円未満	10億～100億円未満	不明
合計		101	11	6	9	6	69
		100.0	10.9	5.9	8.9	5.9	68.3
F属性	企業	50	5	6	7	6	26
		100.0	10.0	12.0	14.0	12.0	52.0
	大学	44	5	0	0	0	39
		100.0	11.4	0.0	0.0	0.0	88.6

		全体	Q7 年間研究開発費						
			なし	～1,000万円未満	1,000万～1億円未満	1億～10億円未満	10億～100億円未満	100億円以上	不明
合計		101	11	9	5	9	4	2	61
		100.0	10.9	8.9	5.0	8.9	4.0	2.0	60.4
F属性	企業	50	7	5	4	6	4	2	22
		100.0	14.0	10.0	8.0	12.0	8.0	4.0	44.0
	大学	44	2	4	1	2	0	0	35
		100.0	4.5	9.1	2.3	4.5	0.0	0.0	79.5

		全体	Q8 研究開発人員							
			0人	1～4人	5～9人	10～19人	20～49人	50～99人	100人以上	不明
合計		101	10	15	7	4	6	1	9	49
		100.0	9.9	14.9	6.9	4.0	5.9	1.0	8.9	48.5
F属性	企業	50	6	7	4	2	3	1	6	21
		100.0	12.0	14.0	8.0	4.0	6.0	2.0	12.0	42.0
	大学	44	2	7	2	2	3	0	3	25
		100.0	4.5	15.9	4.5	4.5	6.8	0.0	6.8	56.8