独立行政法人**情報処理推進機構**

〒113-6591
東京都文京区本駒込2-28-8　文京グリーンコートセンターオフィス16階
http://www.ipa.go.jp/

ＳＳＬサーバ設定状況等の調査報告書

２０１２年１２月

目 次

1. 調査業務の実施方針等

1.1 背景・目的

インターネットの普及に伴い、インターネットを用いた電子商取引の利用も拡大している。経済産業省の平成 22 年度電子商取引に関する市場調査では、平成 22 年のコンシューマ向け電子商取引市場規模は前年比 20%増の 5.3 兆円規模と推定されている。また、日本においては少子高齢化に伴い、買い物弱者に対する買い物支援サービス等も提供されることから、オンラインショッピングのみならず、インターネットバンキング等の利活用が促進されることが考えられ、インターネットを用いた電子商取引は今後も拡大することが想定されている。これらでやり取りされる重要な情報を守るための技術の重要性も認識されている。インターネットを安心して利用するための代表的な技術としては、SSL（Secure Socket Layer）プロトコルによる通信の秘匿化がある。

一方、インターネットを用いて重要な情報をやり取りする一般コンシューマは、SSL プロトコルを意識する・しないに関わらず利用している場合や、「SSL を採用し、重要な情報を秘匿化し守っている」という告知のみを信用し、SSL プロトコルが安全に機能していることを確認しない場合も考えられる。このため、SSL プロトコルが安全に機能していること調査する必要がある。

本調査では、SSL プロトコルを制御する SSL サーバの設定について調査し、SSL サーバの構築者及び利用者に対して SSL サーバの適切な設定を踏まえた対策や安全な利用に関する指標に資する調査を実施した。

1.2 方針

以上の目的を踏まえ、客観的指標となる目標を以下のように設定する。SSL プロトコルを制御する SSL サーバの設定を調査するうえで重要な項目は、SSL プロトコルに用いられる暗号アルゴリズムの優先度の設定（Cipher suite の優先順位）と SSL サーバ証明書で設定されている暗号アルゴリズムやハッシュ関数及び発行者等の設定情報である。これらを短期間に調査し、SSL サーバの構築者及び利用者に対する SSL プロトコルの安全な利用に関する啓発資料に資する調査を行うために、以下の 4 点の方針を定め調査を実施する。

①SSL サーバ設定の実態を調査するために、調査対象となる SSL サーバの管理者に対する事前告知を行わず、真の実態を調査する。また、SSL サーバの管理者に事前告知を行わないため、調査対象となる SSL サーバの負荷を考慮し、調査手法が安全であることを確認した後に調査を実施する。また、東日本地域では、大震災の影響によって、本稼動の設定では異なる SSL サーバが存在する可能性があること、また、調査過程で重大な瑕疵を発見した場合の連絡が滞ることも考えられるため、災害地域については、調査対象から除外する。

②近年のインターネット利用端末として普及しているスマートフォンに関する調査については、他のプラットフォームの調査結果を基に、特徴的な業種及びサービスに対して調査を実施する。

③SSL サーバ証明書については、発行者の記載・設定が SSL サーバを管理する企業や団体である場合と、SSL サーバの管理・運用を委託した企業である場合がある。SSL サーバの管理・運用を委託した企業が SSL サーバ証明書に記載されている場合では、一般コンシューマは正しい発行者であるか否かを確認することが出来ない場合もある（このような問題はサイト名不一致問題等とも呼ばれる）。これらの調査結果については、必要に応じて SIer や有識者との意見交換を行い SSL サーバの安全な設定の啓発に資する指標（案）を提供する。

④SSL サーバの調査結果及び SSL プロトコルの安全性評価については、ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度（JISEC）の実務経験者がレビューを行い、客観的及び定性的な観点を踏まえた報告書を作成する。

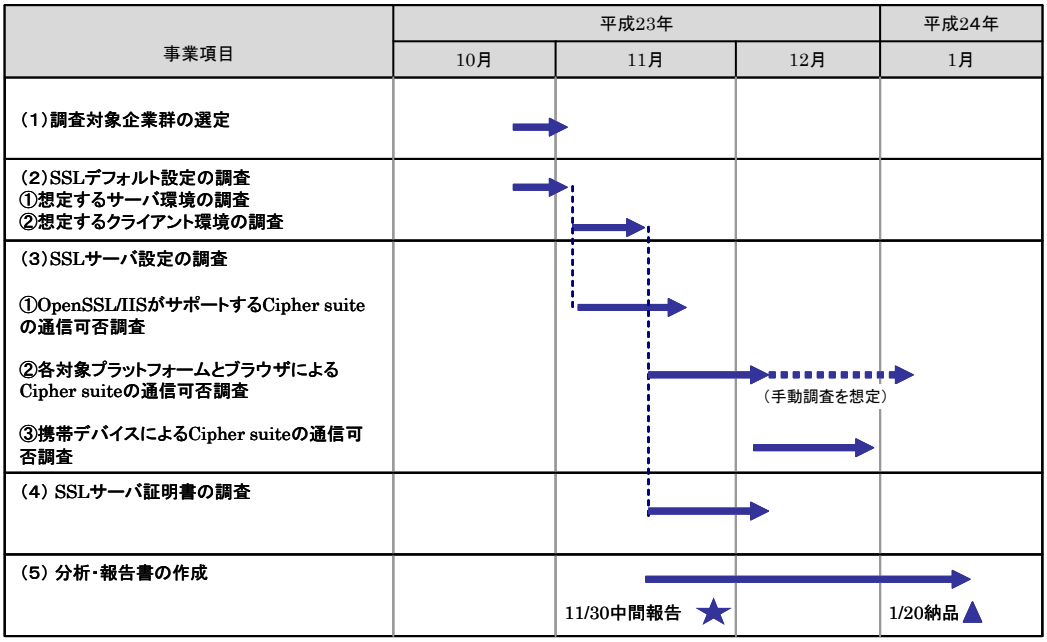
1.3　実施作業内容

本調査の概要を以下に示す。はじめに、調査対象となる SSL サーバ（300 台）の特定、及びサーバ環境やクライアント環境の特定を行い、事前調査を実施した。この事前調査では、SSL サーバやクライアント環境のデフォルト設定等を調査し、SSL サーバの設定状況の調査を効率的且つ、安全に調査が実施できるように調査を行った。続いて、調査対象と特定した SSL サーバに対して、SSL サーバの設定状況を調査した。最後に、調査結果を基に、分析を行い、SSL サーバの構築者及び利用者に対して SSL サーバの適切な設定や SSL プロトコルが安全に機能しているかについてまとめた。

図表：実施作業概要

1.4　実施スケジュール及び事業の実現性

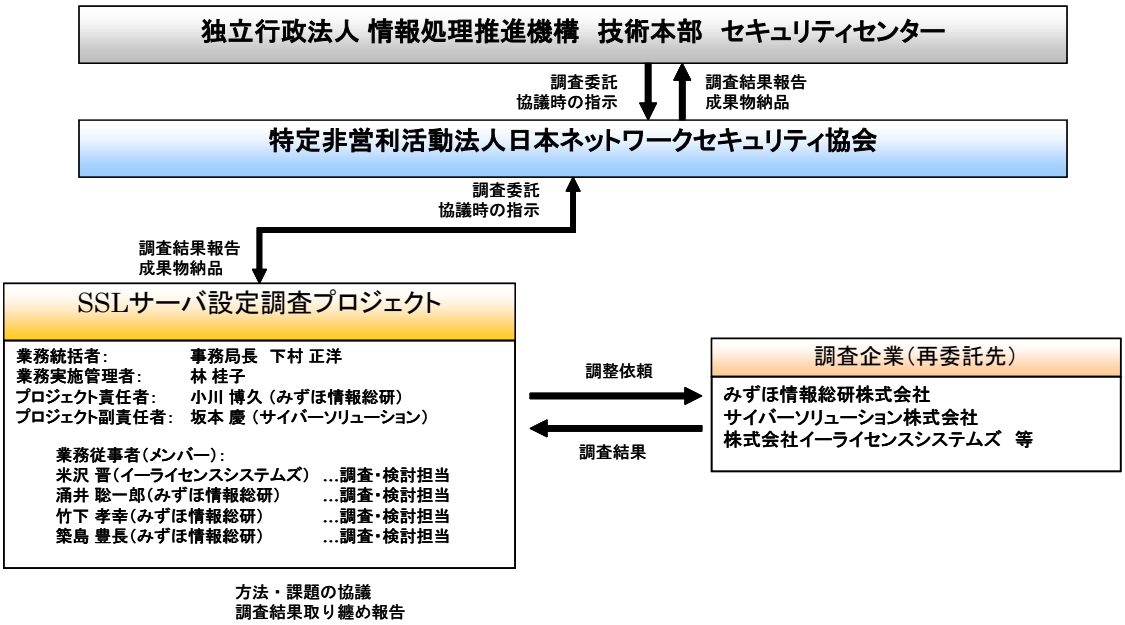
前述した調査内容を基に、本業務は以下のスケジュールにて実施した。
なお、下記のスケジュールで示した通り、（２）SSL デフォルト設定の調査と（３）SSL サーバ設定調査の一部を平行して調査を実施し、（３）SSL サーバ設定調査と（４）SSL サーバ証明書の調査を同時に実施し、調査作業の効率化を行った。



図表：実施スケジュール概要

1.4.1　調査実施体制

本調査の実施体制は下図のとおりである。



図表：実施体制図

2. 調査実施方法

2.1 調査対象ＳＳＬサーバの特定

調査対象となるＳＳＬサーバの特定については、以下の観点（選定理由）から３種の業界を特定した。

項目	内容
調査対象業界	以下 A～C の3業界について調査を実施する。 A)金融系 B)物販系 C)非物販系
業界選定理由	A)インターネットを介した電子決済などのサービスが提供され、SSLサーバの詐称等が可能であるかをチェックために SSL サーバの設定調査が重要であること。また、既存の調査研究を踏まえ、経年変化を調査するために必要な業界である。 B)上記と同様に電子決済等のサービスが提供されている業界であるため。 C)上記と同様に電子決済等のサービスが提供されている業界であるため。
SSL サーバ特定方法	インターネットなどの公開情報を基に、企業及び団体について調査し、URLを特定する。
主な情報源	Web 情報(インターネット)

図表：ＳＳＬサーバ選定及び業界選定調査概要

2.1.1 金融系

金融系の調査対象となるＳＳＬサーバについては、詳細分類を７種に詳細化し、そのすべてを調査対象とした。なお、調査対象変更、及び調査方法の妥当性検証も含め、地方銀行の調査対象を 22 追加し、調査実施した。詳細は別紙調査シートを参照。

	詳細分類	対象数 (調査予定数)	調査実施数
1	都市銀行	11	11
2	地方銀行	34	56
3	ネット系	15	15
4	信託系	13	13
5	証券系	12	12
6	キャッシング系	10	10
7	クレジットカード	5	5
	合計	100	122

図表：調査対象ＳＳＬサーバの詳細分類（金融系）

2.1.2 物販系

物販系の調査対象となるＳＳＬサーバについては、詳細分類を１１種に詳細化し、そのすべてを調査対象とした。また、ＳＳＬサーバの調査対象（調査予定対象）と調査実施対象は同一であり、全ての対象について調査実施した。なお、詳細は別紙調査シートを参照。

	詳細分類	対象数 (調査予定数)	調査実施数
1	総合通販	8	8
2	百貨店	7	7
3	音楽・書籍・ゲーム	11	11
4	家電・パソコン・通信	13	13

	詳細分類	対象数 （調査予定数）	調査実施数
5	ファッション	14	14
6	キッズ・ベビー・玩具	10	10
7	ギフト・お花・ペット	13	13
8	インテリア・日用雑貨	7	7
9	スポーツ・アウトドア	6	6
10	美容・健康	8	8
11	その他	3	3
	合計	100	100

図表：調査対象ＳＳＬサーバの詳細分類（物販系）

2.1.3　非物販系

非物販系の調査対象となるＳＳＬサーバについては、詳細分類を 16 種に詳細化し、そのすべてを調査対象とした。また、ＳＳＬサーバの調査対象数（調査予定対象数）は 100 であるが、調査実施対象数は調査内容によって異なり、102 及び 103 である。調査対象数（調査予定対象数）と査実施対象数の相違について以下に説明する。

- **詳細分類「５．人材紹介・転職・就職」の内、1 つについて、調査ツールである nmap による HTTP 接続がリセットされる状況があり、検査を続行できなかったため、「５．人材紹介・転職・就職」の予備候補に調査対象を変更し、調査を実施した。（下表の赤色枠）なお、この調査対象については、Cipher suite の調査は実施できなかったが、SSL 証明書を調査は実施した。**
- **また、同現象を確認すること及び調査方法の妥当性検証も含め、予備候補を設定していた「３．旅行・宿泊予約」及び「１３．クーポン共同購入サイト」について、調査対象を各々1 つ（合計 2）追加変更し、調査を実施した。（下表の黄色枠）**

このため、接続可能な Cipher suite の調査実施数は 102 であり、クライアント環境による調査及び SSL 証明書の調査実施数は、103 である。
なお、詳細は別紙調査シートを参照。

	詳細分類	対象数 （調査予定数）	調査実施数 （接続可能な Ciper suite）	調査実施数 （クラウアント環境による調査/SSL 証明書調査）
1	不動産	3	3	3
2	運輸・輸送	12	12	12
3	旅行・宿泊予約	7	8	8
4	比較サイト・口コミサイト・Q＆Aサイト	7	7	7
5	人材紹介・転職・就職	7	7	8
6	WEB サービス	12	12	12
7	チケット予約	4	4	4
8	音楽配信・映像配信・電子書籍	5	5	5
9	アンケートサイト・ポイントサイト	6	6	6
10	レンタカー・タクシー予約	6	6	6
11	教育（e-Learning、オンライン英会話）	6	6	6
12	報道機関	5	5	5
13	クーポン共同購入サイト	8	9	9
14	ホテル（国内）	3	3	3
15	ホテル（海外）	3	3	3
16	その他	6	6	6
	合計	100	102	103

図表：調査対象ＳＳＬサーバの詳細分類（非物販系）

2.2　ＳＳＬデフォルト設定の調査

今回、調査を行った調査対象プラットフォーム（サーバ、クライアント）を示す。

一部プラットフォームにおいては、調査時点において最新のプラットフォームでテストを行った関係上、仕様書と異なるバージョンが存在する。また、「Windows 2008 Server」においては、現時点において入手が困難であったため、調査の目的を鑑みて影響がない「Windows Web Server 2008」にて調査を行った。これらの該当箇所について、下表に赤字斜体にて記載する。

No	プラットフォーム名	クライアント	サーバ
1	Windows XP Service pack 3	○	－
2	Windows Vista Service pack 2	○	－
3	Windows 7 Home Premium Service pack 1	○	－
4	Windows 7 Professional Service pack 1	○	－
5	Mac OS X	○	－
6	Ubuntu 11.10 Desktop *(Ubuntu 11.04)*	○	－
7	Ubuntu 11.10 Server *(Ubuntu 11.04)*	－	○
8	Red Hat Enterprise Linux 5.4	－	○
9	Red Hat Enterprise Linux 6.1 *(Red Hat Enterprise Linux 6)*	－	○
10	Windows Server 2003 Service Pack 2	－	○
11	Windows Web Server 2008 Service Pack 2 *(Window Server 2008 Service Pack 2)*	－	○
12	Windows Server 2008 R2 Service Pack 1	－	○

図表：調査対象プラットフォーム

2.2.1 調査項目

仕様書で示された各プラットフォームにおける調査項目を示す。主に、サーバ環境における利用が考えられる OpenSSL、Internet Information Services (IIS)については、サポートする Cipher suite の一覧を調査した。また、クライアント環境における利用が考えられる各種のブラウザについては、サポートする Cipher suite の一覧と、デフォルト設定時の Cipher suite の優先順位を調査した。

一部調査項目（ブラウザ）においては、調査時点において最新の調査項目でテストを行った関係上、仕様書と異なるバージョンが存在する。また、一部の OpenSSL については、該当する OpenSSL がプラットフォーム側でサポートされていない（パッケージとして提供されていない）ため、それぞれソースからインストールして調査を実施した。これらの該当箇所について、下表に赤字斜体にて記載する。

No	調査項目	サポートする Cipher suite の一覧	デフォルト設定時の Cipher suite の優先順位
1	Internet Explorer (IE7)	○	○
2	Internet Explorer (IE8)	○	○
3	Internet Explorer (IE9)	○	○
4	Firefox (Firefox 3.6)	○	○
5	Firefox (Firefox 7) *(Firefox 4, Firefox 5.0)*	○	○
6	Google Chrome (Chrome 15) *(Chrome 12)*	○	○
7	Opera (Opera 11.52) *(Opera 11.50)*	○	○
8	Safari (Safari 5.1.1) *(Safari 5)*	○	○
9	OpenSSL (OpenSSL 0.9.8e/0.9.8r) *(OpenSSL 0.9.8r)*	○	－
10	OpenSSL (OpenSSL 1.0.0e) *(OpenSSL 1.0.0d)*	○	－
11	Internet Information Services 6.0 (IIS 6.0)	○	－
12	Internet Information Services 7.0 (IIS 7.0)	○	－
13	Internet Information Services 7.5 (IIS 7.5)	○	－

図表：調査項目

2.2.2　調査対象プラットフォームと調査項目

本調査では、上記①で示した調査対象プラットフォームのクライアント及びサーバに基づき、上記②で示した調査項目におけるデフォルトの設定調査を行った。概要を下表に示す。下表では、調査対象プラットフォームを横軸（行）に記載し、調査項目を縦軸（列）に記載し、交差した項目で調査対象に該当するものに番号（クライアント：cXX、サーバ：sXX）を付与した。

- クライアントの調査としては、調査対象プラットフォーム（１～１２）及び調査項目（１～８）のうち３９種類を調査した。
- サーバの調査としては、調査対象プラットフォーム（７～１２）及び調査項目（９～１３）のうち１５種類を調査した。

調査対象プラットフォーム ＼ 調査項目		Internet Explorer (IE7)	Internet Explorer (IE8)	Internet Explorer (IE9)	Firefox (Firefox 3.6)	Firefox (Firefox 7/8) *(Firefox 4, Firefox 5.0)*	Google Chrome (Chrome 15) *(Chrome 12)*	Opera (Opera 11.52) *(Opera 11.50)*	Safari (Safari 5.1.1) *(Safari 5)*	OpenSSL (OpenSSL 0.9.8e/r) *(OpenSSL 0.9.8r)*	OpenSSL (OpenSSL 1.0.0e) *(OpenSSL 1.0.0d)*	Internet Information Services (IIS) (IIS 6.0)	Internet Information Services (IIS) (IIS 7.0)	Internet Information Services (IIS) (IIS 7.5)
		1	2	3	4	5	6	7	8	9	10	11	12	13
1	Windows XP Service pack 3	c1	c3		c10	c16(v7) c16(v8)	c22	c28	c34					
2	Windows Vista Service pack 2	c2	c4	c7	c11	c17	c23	c29	c35					
3	Windows 7 Home Premium Service pack 1		c5	c8	c12	c18	c24	c30	c36					
4	Windows 7 Professional Service pack 1		c6	c9	c13	c19	c25	c31	c37					
5	Mac OS X				c14	c20	c26	c32	c38					
6	Ubuntu 11.10 Desktop *(Ubuntu 11.04)*				c15	c21	c27	c33						
7	Ubuntu 11.10 Server *(Ubuntu 11.04)*									s1	s7			
8	Red Hat Enterprise Linux 5.4									s2	s8			
9	Red Hat Enterprise Linux 6.1 *(Red Hat Enterprise Linux 6)*									s3	s9			
10	Windows Server 2003 Service Pack 2									s4	s10	s13		
11	Windows Web Server 2008 Service Pack 2 *(Window Server 2008 Service Pack 2)*									s5	s11		s14	
12	Windows Server 2008 R2 Service Pack 1									s6	s12			s15

図表：調査対象プラットフォームと調査項目について

2.2.3　ＳＳＬデフォルト設定調査の実施方法

上記２．２．２に示す各調査（クライアント及びサーバの SSL デフォルト設定の調査）の実施方法を以下に示す。調査結果の詳細は付録１及び付録２をご参照。

● サーバの SSL デフォルト設定調査（s1～s12：OpenSSL）

１．各調査対象プラットフォーム上に導入された調査項目（OpenSSL）にて以下のコマンドを発行し、当該調査項目がデフォルトでサポートしている Cipher Suite の一覧を取得する。

＜コマンド＞
openssl ciphers –v

※ 導入されている OpenSSL にてデフォルトで利用可能な Cipher Suite の一覧を暗号強度順に表示するコマンド

＜出力結果の例：s1（Ubuntu 11.10 Server 上の OpenSSL 0.9.8r）＞

```
root@ubuntu-11:/tmp/openssl-0.9.8r$ /usr/local/ssl/bin/openssl version
OpenSSL 0.9.8r 8 Feb 2011
root@ubuntu-11:/tmp/openssl-0.9.8r$ /usr/local/ssl/bin/openssl ciphers -v
DHE-RSA-AES256-SHA      SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
DHE-DSS-AES256-SHA      SSLv3 Kx=DH       Au=DSS  Enc=AES(256)  Mac=SHA1
AES256-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
EDH-RSA-DES-CBC3-SHA    SSLv3 Kx=DH       Au=RSA  Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA    SSLv3 Kx=DH       Au=DSS  Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA            SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
DES-CBC3-MD5            SSLv2 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=MD5
DHE-RSA-AES128-SHA      SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
DHE-DSS-AES128-SHA      SSLv3 Kx=DH       Au=DSS  Enc=AES(128)  Mac=SHA1
AES128-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
IDEA-CBC-SHA            SSLv3 Kx=RSA      Au=RSA  Enc=IDEA(128) Mac=SHA1
IDEA-CBC-MD5            SSLv2 Kx=RSA      Au=RSA  Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5             SSLv2 Kx=RSA      Au=RSA  Enc=RC2(128)  Mac=MD5
RC4-SHA                 SSLv3 Kx=RSA      Au=RSA  Enc=RC4(128)  Mac=SHA1
RC4-MD5                 SSLv3 Kx=RSA      Au=RSA  Enc=RC4(128)  Mac=MD5
RC4-MD5                 SSLv2 Kx=RSA      Au=RSA  Enc=RC4(128)  Mac=MD5
EDH-RSA-DES-CBC-SHA     SSLv3 Kx=DH       Au=RSA  Enc=DES(56)   Mac=SHA1
EDH-DSS-DES-CBC-SHA     SSLv3 Kx=DH       Au=DSS  Enc=DES(56)   Mac=SHA1
DES-CBC-SHA             SSLv3 Kx=RSA      Au=RSA  Enc=DES(56)   Mac=SHA1
DES-CBC-MD5             SSLv2 Kx=RSA      Au=RSA  Enc=DES(56)   Mac=MD5
EXP-EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH(512)  Au=RSA  Enc=DES(40)   Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH(512)  Au=DSS  Enc=DES(40)   Mac=SHA1 export
EXP-DES-CBC-SHA         SSLv3 Kx=RSA(512) Au=RSA  Enc=DES(40)   Mac=SHA1 export
EXP-RC2-CBC-MD5         SSLv3 Kx=RSA(512) Au=RSA  Enc=RC2(40)   Mac=MD5  export
EXP-RC2-CBC-MD5         SSLv2 Kx=RSA(512) Au=RSA  Enc=RC2(40)   Mac=MD5  export
EXP-RC4-MD5             SSLv3 Kx=RSA(512) Au=RSA  Enc=RC4(40)   Mac=MD5  export
EXP-RC4-MD5             SSLv2 Kx=RSA(512) Au=RSA  Enc=RC4(40)   Mac=MD5  export
```

サーバ（OpenSSL）のデフォルト設定において利用可能な Cipher Suite の一覧とその詳細（SSL のバージョン、鍵交換方式、認証方式、共通化暗号化方式、メッセージ認証方式等）が出力される。

● **サーバの** SSL **デフォルト設定調査（**s13～s15：IIS**）**

１. Microsoft **社の提供する同社製品に関するソフトウェア開発者を支援するサービスである「**MSDN(Microsoft Developers Network) **」を基に、各調査対象プラットフォーム上に導入された調査項目（**IIS**）でサポートされている** Cipher Suite **について調査を行う。**
２. **各調査対象プラットフォームのレジストリ情報を基に、デフォルト設定において利用可能な** SSL **のバージョンや暗号化** NULL **設定の利用可否を調査する。調査結果と上記** 1.**にて調査した** Cipher Suite **との対応関係を整理することにより、デフォルト設定にて利用可能な** Cipher Suite **を特定する。**
３. **各調査対象プラットフォーム上の調査項目（**IIS**）において、一般的な自己証明書の作成方法にて** SSL **対応ウェブサーバの設定を行い、以下のツールを用いて上記** 2.**で特定した** Cipher Suite **について部分的に補足確認を行う。**

＜利用したツール＞

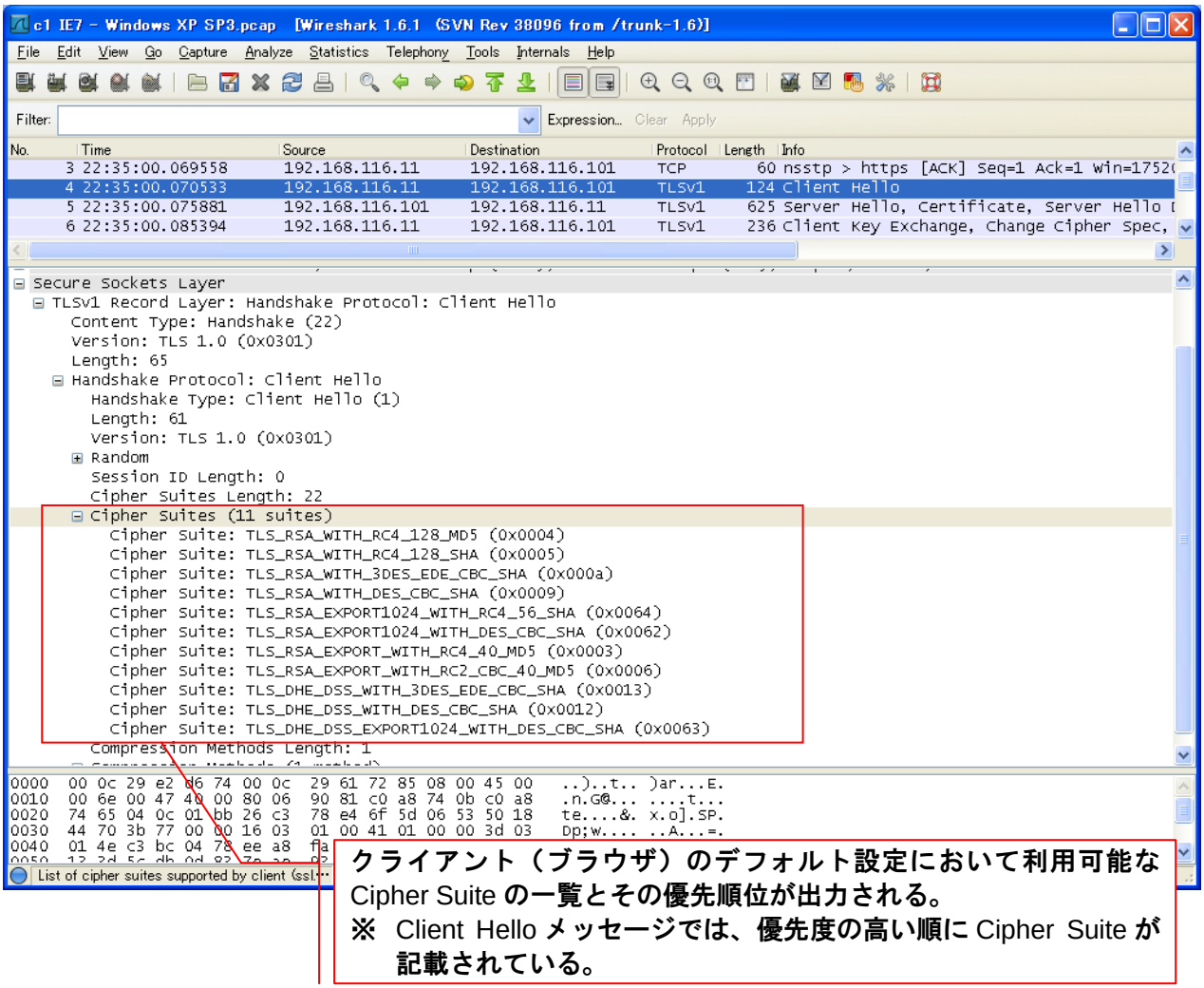
- Nmap (http://nmap.org/)
  - SSL3.0/TLS1.0 **を調査する場合：**ssl-enum-ciphers.nse **（**http://nmap.org/nsedoc/scripts/ssl-enum-ciphers.html**）**
  - SSL2.0 **を調査する場合：**sslv2.nse **（**http://nmap.org/nsedoc/scripts/sslv2.html**）**
- THCSSLCheck (http://www.thc.org/root/tools/)
- sslscan(https://www.titania-security.com/labs/sslscan)

●クライアントの SSL デフォルト設定調査（c1～c38）

1．各調査対象プラットフォーム上の調査項目（ブラウザ）を用いて、本調査用に構築した SSL 対応ウェブサーバにアクセスする。

2．SSL 対応ウェブサーバとの通信内容（SSL Handshake Protocol）をパケットキャプチャツール（Wireshark）にて取得し、Client Helo メッセージの内容から当該 SSL 通信で用いられる Cipher Suite の種類と優先順位を調査する。

＜出力結果の例：c1（Windows XP Service pack 3 上の Internet Explorer 7）＞



クライアント（ブラウザ）のデフォルト設定において利用可能な Cipher Suite の一覧とその優先順位が出力される。

※ Client Hello メッセージでは、優先度の高い順に Cipher Suite が記載されている。

2.2.4 ＳＳＬデフォルト設定の調査実施期間

SSL サーバ設定の調査は、平成 23 年 11 月～平成 24 年 1 月に実施した。

2.3 ＳＳＬサーバ設定の調査

ＳＳＬサーバ設定の調査は、２.１節の「調査対象 SSL サーバの選定」によって選定された SSL サーバへアクセスを行い、対象サーバの SSL 設定状況を調査するものである。

2.3.1 調査項目

仕様書で示された調査項目として以下の 2 つの調査を行った。

２.２節で調査した OpenSSL または IIS の少なくとも一方がサポートする全ての Cipher suite について、２.１節で特定した SSL サーバとの通信可否を確認し、Cipher suite が利用可能であるかどうかを調査した(以下、Cipher suite の組み合わせ調査と記載)。

また、２.２.２の各調査対象プラットフォームにおいて、調査項目で挙げたブラウザがどの Cipher suite で SSL サーバとの通信を確立するかについて調査した(以下、デフォルト設定での接続調査と記載)。

調査で想定したクライアント環境については、下表の OS 及びブラウザである。

	Firefox 3	Firefox 7	Firefox 8	Google Chrome	Internet Explorer 7	Internet Explorer 8	Internet Explorer 9	Opera	Safari
MacOS X	cx1	cx2	cx3	cx4	–	–	–	cx5	cx6
Ubuntu 11	cx7	cx8	cx9	cx10	–	–	–	cx11	–
Windows 7 Home	cx12	cx13	cx14	cx15	–	cx16	cx17	cx18	cx19
Windows 7 Ultimate	cx20	cx21	cx22	cx23	–	cx24	cx25	cx26	cx27
Windows Vista	cx28	cx29	cx30	cx31	cx32	cx33	cx34	cx35	cx36
Windows XP	cx37	cx38	cx39	cx40	cx41	–	cx42	cx43	cx44

図表：想定クライアント環境の OS 及びブラウザ

2.3.2 調査実施環境

各調査対象プラットフォームの環境を用意して調査を行った。Windows 環境については IE のバージョンが複数存在し、かつ共存できないため、各バージョンごとに個別の環境を用意して調査を行った。ブラウザによる対象サイトへのアクセス自動化および結果の集計等に必要なプログラムは Perl で開発した。

2.3.3 調査方法

ＳＳＬサーバ設定の調査については、（１）cipher suite の組み合わせ調査と（２）デフォルト設定での接続調査を行った。各調査の実施方法を以下に示す。各調査結果の詳細は別紙調査シートを参照のこと。

（１）cipher suite の組み合わせ調査

調査にあたっては、２.２.３と同様のツールを使用した。その際に、接続を試みる Cipher suite を OpenSSL もしくは IIS のいずれかがサポートしているものに限定するため、nmap 内部で使用するファイル(NSE: Nmap Scripting Engine)をカスタマイズして使用した。

手順は以下：

1. tcpdump を使用してパケットキャプチャを実施し(ポート 443 のみフィルタして取得)、結果データを PCAP 形式でファイルに保存した。パケットキャプチャは、以下の 2 を実行している間取得し、1 サイトの調査ぼとに別ファイルで保存した。
2. SSLv3 での調査としては、nmap を使用して調査対象サーバへアクセスし、nmap の出力結果からサーバが提示した Cipher suite を取得した。コマンドは以下の通り：

nmap -d --script=ssl-enum-ciphers -p 443 “接続先サーバ名”

調査対象サーバで使用可能な Cipher Suite は、nmap の実行結果では以下のように表示され確認できる(太字部分が Cipher suite の値)。

```
PORT    STATE SERVICE REASON
443/tcp open  https   syn-ack
| ssl-enum-ciphers-custom-server:
|   SSLv3
|     Ciphers (8)
|       0x2f    TLS_RSA_WITH_AES_128_CBC_SHA
|       0x3     TLS_RSA_EXPORT_WITH_RC4_40_MD5
|       0x35    TLS_RSA_WITH_AES_256_CBC_SHA
|       0x4     TLS_RSA_WITH_RC4_128_MD5
|       0x5     TLS_RSA_WITH_RC4_128_SHA
|       0x6     TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
|       0x9     TLS_RSA_WITH_DES_CBC_SHA
|       0xa     TLS_RSA_WITH_3DES_EDE_CBC_SHA
|     Compressors (1)
|       uncompressed
```

3. 同様に SSLv2 での調査としては、nmap を使用して調査対象サーバへアクセスし、nmap の出力結果からサーバが提示した Cipher suite を取得した。コマンドは以下の通り：

nmap -d -sV -sC -p 443 “接続先サーバ名”

調査対象サーバで使用可能な Cipher Suite は、nmap の実行結果では以下のように表示され確認できる(太字部分が Cipher suite の値)。

```
PORT    STATE SERVICE  REASON  VERSION
443/tcp open  ssl/http syn-ack Microsoft IIS httpd 6.0
| sslv2: server still supports SSLv2
|       SSL2_DES_192_EDE3_CBC_WITH_MD5
|       SSL2_RC2_CBC_128_CBC_WITH_MD5
|       SSL2_RC4_128_WITH_MD5
|       SSL2_RC4_64_WITH_MD5
|       SSL2_DES_64_CBC_WITH_MD5
|_      SSL2_RC4_128_EXPORT40_WITH_MD5
```

（2）デフォルト設定での接続調査

２.２.２の図表にある調査対象プラットフォームのうち、クライアント環境(プラットフォーム 6 種類)でブラウザを使用して調査対象サーバにアクセスして調査を行った。結果については、前項と同様にパケットキャプチャを実施して取得した。

手順は以下：

1. サイトの一覧 CSV から検査リストを作成
2. 以下の一連の動作をおこなうプログラムを作成し、実行
   - tcpdump コマンドを使用してパケットキャプチャを開始(ポート 443 のみフィルタして取得)
   - アクセスする URL を指定してブラウザを起動
   - 一定時間待ち、ブラウザを終了
   - パケットキャプチャを終了
3. 上記で取得したパケットキャプチャデータから使用した Cipher suite を特定

※ 結果抽出方法について

結果の抽出にあたり、パケットキャプチャにて取得した結果データより選択された Cipher suite を確認するために使用した手順を以下に示す。

手順としては、パケットキャプチャしたデータを以下の方法等にて解析し、実行された SSL ハンドシェイクの内容を確認する。

A) Wireshark を使用してパケットキャプチャしたデータを開き、デコード画面で内容を確認する。

B) Wireshark に付属の tshark コマンド(Wireshark のコマンドライン版)を使用し、以下のように実行して該当の SSL ハンドシェイク部分の内容を確認する。

tshark –n –V –r “キャプチャデータファイル”

このコマンドの出力内容から、SSL ハンドシェイクに含まれる「Server Hello」を検索し、その近傍に記載されている「Cipher Suite」の内容をもってこの結果とする。以下に当該部分のデコード結果内容を示す(斜体部分が検索対象文字列、太字部分が Cipher suite の値)。

```
Secure Socket Layer
   TLSv1 Record Layer: Handshake Protocol: Multiple Handshake Messages
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 5156
      Handshake Protocol: Server Hello
         Handshake Type: Server Hello (2)
         Length: 70
         Version: TLS 1.0 (0x0301)
         Random
            gmt_unix_time: Jan  1, 1970 09:01:18.000000000
            random_bytes: 848FE0A952B88F0B303792157F2BC93B931BC1446E8963E4...
         Session ID Length: 32
         Session ID: 0000180BFF6911B728363BBBA7162CE2949E7C1558585858...
         Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
         Compression Method: null (0)
```

実際の調査では、この Cipher suite の値を抽出して集計するプログラムを作成して行った。

2.3.4 ＳＳＬサーバ設定の調査実施期間

ＳＳＬサーバ設定の調査は、平成２３年１１月～平成２４年１月に実施した。

2.4　ＳＳＬサーバ証明書の調査

ＳＳＬサーバ証明書の調査は、２.３節と同様に、２.１節の「調査対象 SSL サーバの選定」によって選定された SSL サーバへアクセスを行い、対象サーバの SSL サーバ証明書を調査するものである。

2.4.1　ＳＳＬサーバ証明書の調査項目

調査対象（3 業界合計で 325 サーバ）に対して、以下に示す項目の調査を行った。

・発行日（※1）
・失効日（※1）
・署名アルゴリズム
・署名長
・公開鍵暗号
・公開鍵長
・発行者情報
・サブジェクト（※2）
・EV-SSL の有無

※1 タイムゾーンは GMT 発行日と失効日の間の期間をもって有効期間とする。
※2 当該 SSL サーバ証明書が EV-SSL 証明書である場合、各証明書発行者の定めるオブジェクト識別子(OID)がサブジェクトに含まれるため、参考情報として調査を行った。

2.4.2　調査実施環境

２.３.２と同じ環境を使用して調査を行った。調査対象サイトへのアクセスおよび結果の集計等に必要なプログラムは Perl で開発した。

2.4.3　調査方法

各調査の実施方法を以下に示す。調査結果の詳細は別紙調査シートを参照のこと。

調査にあたっては、まず OpenSSL の s_client 機能を使用して SSL サーバ証明書を取得し、その SSL サーバ証明書から各調査項目を抽出するためのプログラムを作成して行った。

EV-SSL については、調査対象サーバに対してブラウザを使用してアクセスし、アドレスバーの表示(アドレスバーが緑色で表示されるなど)で確認を行った。また、この結果とサブジェクトに特定の OID が含まれるものが一致することを確認したが、特定の OID が含まれることが EV-SSL であると断定できるかどうかは不明である。

2.4.4　ＳＳＬサーバ証明書の調査実施期間

ＳＳＬサーバ証明書の調査実施期間は、ＳＳＬサーバ設定の調査と同時に実施したため、２.３.４と同時期の平成２３年１１月～平成２４年１月に実施した。

2.5　携帯デバイスを用いた調査

携帯デバイス（スマートフォン等を含む）に対応している SSL サーバに対して、Cipher suite の接続調査を行った。具体的には、各携帯デバイス（スマートフォン等を含む）として、iOS、Android 等の搭載デバイスを用いて対象の SSL サーバに対して接続調査を行った。本調査も２.３節の調査と同様に、各携帯デバイス（スマートフォン等を含む）のデフォルト設定において、WiFi を介して SSL 通信を行う際の Cipher suite の選択を確認した。
なお、調査対象の SSL サーバについては、以下の調査概要等の通りである。

項目	内容
調査対象	調査対象の SSL サーバについて以下を分類して調査し、合計 10 サイトを調査した。 ・PC 等を対象とした一般的な Web サイト ・携帯デバイス向けの Web サイト ・携帯デバイス用アプリによって接続するサイト
対象の携帯デバイス	・Android（Version 2.3.2、2.3.3、2.3.4、2.3.5、3.2） ・iPhone（Version 4.3.5、5.0）
調査項目	・対象となる SSL サーバに対して、携帯デバイスのデフォルト設定において通信確立した Cipher suite を調査する。
調査ツール類	・ノート PC に Wifi のアクセスポイントを設定（ツール名：CONNECTIFY LITE）。 ・上記の設定を行ったノート PC にインストールしたパケットキャプチャ（Wireshark）を用いて上記の調査項目データを確認する。

図表：調査対象の選定及び調査概要等

3. 調査結果

3.1 調査結果報告の観点

本調査では、調査対象となる 300 サーバに対して、Cipher suite の設定を調査するものであり、調査報告については膨大な量から調査目的に資する項目について調査対象全体を俯瞰できる形式でとりまとめる必要がある。そのため、本調査における調査結果のとりまとめ方法と分析の観点について示す。

3.1.1 本調査結果のとりまとめについて

本調査では、オンラインショッピングやインターネットバンキング、ネットトレードなどのサービスを提供している SSL サーバの設定状況について、特に安全性の確認を行うことに主眼があるため、仕様書に示された以下の 3 項目について報告する。

（１）安全性が不十分な暗号アルゴリズムが選択・利用状況について（仕様書 2.2(1)に該当）

各種の Cipher suite で利用している暗号アルゴリズムについては、安全性が不十分であると判断されている暗号アルゴリズムが含まれている。これらの選択及び利用状況を調査報告に含める。

具体的には、安全な利用に関する各種ガイドラインなどの指標や推奨を基に、安全である暗号アルゴリズムと推奨されていない暗号アルゴリズムに分けて整理する。例えば、ＳＳＬで利用できる Cipher suite に関する指標や推奨については、参照文献の[3] 、[5] 等に示されているが、特に、CRYPTREC が 2008 年に発行した「電子政府推奨暗号の利用方法に関するガイドブック」[4] は、SSL/TLS に関する国内初の公式なガイドラインであり、MD5、RC4、DES 及び Triple DES は推奨されていない。

以上のことから、①CRYPTREC のガイドブックで推奨されている暗号アルゴリズムのみで構成された Cipher suite と、②CRYPTREC のガイドブックで推奨されていない暗号アルゴリズムが含まれた Cipher suite に分けて報告する。（下表にこの観点でまとめた表を示す。この表では、①を黄色で示している。）

また、詳細な分類を行う際には、上記の②に分類される推奨されていない暗号アルゴリズムについて以下の 4 種類を含む。

- 輸出規制に対応した安全性の低い暗号アルゴリズムとして、特に鍵長 40bit 以下の暗号アルゴリズム
- ライセンス関連で問題となる暗号アルゴリズム（例えば、IDEA 暗号が含まれる）
- SSL 2.0 で規定されている Cipher suite（この Cipher suite には、上記の詳細分類に該当する暗号アルゴリズム等も含まれる）
- 上記以外で安全性が不十分であると判断されている暗号アルゴリズム

（２）暗号アルゴリズムの世代交代に関する設定及び利用状況（仕様書 2.2(2)に該当）

各種の Cipher suite で利用している暗号アルゴリズムについては、参照文献[2] 、[8] に示された世代交代に関連した暗号アルゴリズムが含まれている。これらの選択及び利用状況を調査報告に含める。

具体的には、AES 暗号と 3DES(Triple DES)暗号の対比及び、RSA 鍵長 1,024bit と RSA 鍵長 2,048bit 等の対比を含んだ形式で報告する。

（３）SSL サーバ証明書の適切な利用状況を把握できること（仕様書 2.2(3)に該当）

SSL サーバ証明書の適切な利用状況については、失効日を過ぎた証明書を利用していないこと等を報告する。

以下に、前述した観点（１）で示した分類の詳細を示す。下表は、Cipher suite No1～71 を例に、推奨された共通鍵暗号アルゴリズム及びメッセージ認証及び NIST の推奨などをまとめた表である。非推奨アルゴリズム等の列では、（１）で分類すべき、推奨された共通鍵暗号アルゴリズム及びメッセージ認証である MD5、RC4、DES、Triple DES（表内では 3DES）、IDEA を示している。同様に SSL/TLS Version 等の列で、SSL 2.0 とその他の SSL/TLS を示している。

また、SP800-131A の列では、米国立標準技術研究所 NIST（National Institute of Standards and Technology）が 2011 年 1 月に公表したガイドラインである SP800-131A の内容を示している。SP800-131A は、暗号利用・移行計画である SP800-57 の一部修正した内容であり、暗号アルゴリズム及び鍵長によって、以下の 3 種類に分類している。

①Acceptable
②2010 年末迄 Acceptable、2013 年末迄 Deprecated、2014 年 1 月以降は Legacy-use
（署名生成・署名検証以外の利用については Acceptable）
③2010 年末迄 Acceptable、2015 年末迄 Deprecated、2016 年以降は Legacy-use
（復号以外の利用については Disallowed）

本調査では、Cipher suite について調査するが、鍵交換及び認証に関する鍵長については、SSL サーバ証明書の項目で調査するため、SP800-131A に関連する共通鍵暗号アルゴリズムとメッセージ認証を表に示している。また、具体的な記載及び分類は以下の通りである。

SP800-131A 列の共通鍵暗号化では、以下のように記載している。

- Acceptable ：SP800-131A で Acceptable であるアルゴリズム
- “—”：SP800-131A で記載のないアルゴリズム（NIST の標準アルゴリズムでない）

これらの分類の結果、共通鍵暗号アルゴリズムとメッセージ認証における CRYPTREC のガイドブックと NIST SP800-131A の差分は、3DES(Triple DES)暗号のみであり、下表の色分けは以下の通りである。

- 灰色：CRYPTREC 及び NIST の双方で推奨されていない共通鍵暗号アルゴリズムとメッセージ認証（SEED は日本国として推奨されていないため灰色で示す）
- 黄色：CRYPTREC 推奨された共通鍵暗号アルゴリズムとメッセージ認証（一部 NIST の推奨アルゴリズムを含む）
- 白色：CRYPTREC で推奨されていないが、NIST で推奨された共通鍵暗号アルゴリズム（具体的には 3DES）

CS-No.	Cipher Suite	SSL/TLS Version	非推奨アルゴリズム等						その他のアルゴリズム		SP800-131A
			MD5	DES40	DES	SEED	IDEA	RC2	3DES	RC4	共通鍵暗号化
CS1	TLS_RSA_EXPORT_WITH_RC4_40_MD5	SSL 3.0 / TLS 1.0	1	0	0	0	0	0	0	1	—
CS2	TLS_RSA_WITH_RC4_128_MD5	SSL 3.0 / TLS 1.0	1	0	0	0	0	0	0	1	—
CS3	TLS_RSA_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	1	—
CS4	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	SSL 3.0 / TLS 1.0	1	0	0	0	0	1	0	0	—
CS5	TLS_RSA_WITH_IDEA_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	1	0	0	0	—
CS6	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0 / TLS 1.0	0	1	1	0	0	0	0	0	—
CS7	TLS_RSA_WITH_DES_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	1	0	0	0	0	0	—
CS8	TLS_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	1	0	Acceptable
CS9	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0 / TLS 1.0	0	1	0	0	0	0	0	0	—
CS10	TLS_DHE_DSS_WITH_DES_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	1	0	0	0	0	0	—
CS11	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	1	0	Acceptable
CS12	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0 / TLS 1.0	0	1	0	0	0	0	0	0	—
CS13	TLS_DHE_RSA_WITH_DES_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	1	0	0	0	0	0	—
CS14	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	1	0	Acceptable
CS15	TLS_KRB5_WITH_DES_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	1	0	0	0	0	0	—
CS16	TLS_KRB5_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	1	0	Acceptable
CS17	TLS_KRB5_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	1	—
CS18	TLS_KRB5_WITH_DES_CBC_MD5	SSL 3.0 / TLS 1.0	1	0	1	0	0	0	0	0	—
CS19	TLS_KRB5_WITH_3DES_EDE_CBC_MD5	SSL 3.0 / TLS 1.0	1	0	0	0	0	0	1	0	Acceptable
CS20	TLS_KRB5_WITH_RC4_128_MD5	SSL 3.0 / TLS 1.0	1	0	0	0	0	0	0	1	—
CS21	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA	SSL 3.0 / TLS 1.0	0	0	1	0	0	0	0	0	—
CS22	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	1	0	0	—
CS23	TLS_KRB5_EXPORT_WITH_RC4_40_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	1	—
CS24	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5	SSL 3.0 / TLS 1.0	1	0	1	0	0	0	0	0	—
CS25	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5	SSL 3.0 / TLS 1.0	1	0	0	0	0	1	0	0	—
CS26	TLS_KRB5_EXPORT_WITH_RC4_40_MD5	SSL 3.0 / TLS 1.0	1	0	0	0	0	0	0	1	—
CS27	TLS_RSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS28	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS29	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS30	TLS_RSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS31	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS32	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS33	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	—
CS34	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	—
CS35	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	—
CS36	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	1	0	0	0	0	0	—
CS37	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	1	0	0	0	0	0	—
CS38	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	1	—
CS39	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	—
CS40	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	—
CS41	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	—
CS42	TLS_PSK_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	1	—
CS43	TLS_PSK_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	1	0	Acceptable
CS44	TLS_PSK_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS45	TLS_PSK_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS46	TLS_RSA_WITH_SEED_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	1	0	0	0	0	—
CS47	TLS_DHE_DSS_WITH_SEED_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	1	0	0	0	0	—
CS48	TLS_DHE_RSA_WITH_SEED_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	1	0	0	0	0	—
CS49	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	1	—
CS50	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	1	0	Acceptable
CS51	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS52	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS53	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	1	—
CS54	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	1	0	0	0	1	0	Acceptable
CS55	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS56	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS57	TLS_ECDH_RSA_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	1	—
CS58	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	1	0	Acceptable
CS59	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS60	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS61	TLS_ECDHE_RSA_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	1	—
CS62	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	1	0	Acceptable
CS63	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS64	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0	0	0	0	0	0	0	0	0	Acceptable
CS65	SSL_CK_RC4_128_WITH_MD5	SSL 2.0	1	0	0	0	0	0	0	1	—
CS66	SSL_CK_RC4_128_EXPORT40_WITH_MD5	SSL 2.0	1	0	0	0	0	0	0	1	—
CS67	SSL_CK_RC2_128_CBC_WITH_MD5	SSL 2.0	1	0	0	0	0	1	0	0	—
CS68	SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	SSL 2.0	1	0	0	0	0	1	0	0	—
CS69	SSL_CK_IDEA_128_CBC_WITH_MD5	SSL 2.0	1	0	0	0	1	0	0	0	—
CS70	SSL_CK_DES_64_CBC_WITH_MD5	SSL 2.0	1	0	1	0	0	0	0	0	—
CS71	SSL_CK_DES_192_EDE3_CBC_WITH_MD5	SSL 2.0	1	0	1	0	0	0	0	0	Acceptable

図表：推奨された暗号アルゴリズムで構成された Cipher suite

3.1.2　本調査の分析観点について

本調査では、3 種類の業界に対して、２.３.１に示したクライアント環境を用いて調査を行った。そのため、調査の分析軸として以下の 3 つの観点について報告する。

（１）各業界の相違と傾向について

調査対象である 3 つの各業界の中には、業界内固有の標準化や推奨などによって個別の暗号政策が存在する可能性がある（例えば、参照文献[7] で示されている金融分野がこれに該当する）。以上のことから、調査対象である 3 つの各業界について、有意となる相違や傾向に関する分析を調査報告に含める。

（２）OS に関する相違について

調査対象となる一部のブラウザでは、OS で設定した暗号アルゴリズムや Cipher suite を参照し、自動的に SSL で利用する Cipher suite が選択・利用される場合もある。このように OS 設定の影響を受けることが考えられる環境も存在するため、OS ごとに利用している Cipher suite の傾向を分析する。

（３）ブラウザの相違について

上記の（２）OS に関する相違とは別に、調査対象のブラウザでは、OS の影響を受けない場合も考えられる。そのため、ブラウザを軸として傾向を分析する。

なお、以上の分析観点については、（１）の各業界の分析については、業界の SSL サーバ設定に反映されている内容を調査するため、主に、３.３.１、３.３.２、３.３.３で報告し、（２）の OS については、３.３.４で報告し、（３）のブラウザについては、３.３.５で報告する。

3.2　ＳＳＬデフォルト設定調査結果

本節では、２.２で示した SSL デフォルト調査の結果を報告する。

3.2.1　サーバ系設定調査結果

サーバ系環境におけるＳＳＬデフォルト設定は、２.２.２で定めた S1～S15 について調査を実施した。調査の結果、利用可能な Cipher suite は、SSL2.0、SSL3.0/TLS1.0 を含め、71 種類あり、サーバ系環境によってこれらのなかの一部がデフォルト設定で利用できるようになっている。（以下、各々の Cipher suite を SC1～SC71 と略す）71 種類の Cipher suite を下表に示す。

No.	Cipher Suite			SSL/TLS Version
	Hex Value	Cipher Suite	Cipher Suite (OpenSSL Short Name)	
1	0x0003	TLS_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5	SSL 3.0 / TLS 1.0
2	0x0004	TLS_RSA_WITH_RC4_128_MD5	RC4-MD5	SSL 3.0 / TLS 1.0
3	0x0005	TLS_RSA_WITH_RC4_128_SHA	RC4-SHA	SSL 3.0 / TLS 1.0
4	0x0006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	EXP-RC2-CBC-MD5	SSL 3.0 / TLS 1.0
5	0x0007	TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA	SSL 3.0 / TLS 1.0
6	0x0008	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA	SSL 3.0 / TLS 1.0
7	0x0009	TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA	SSL 3.0 / TLS 1.0
8	0x000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	SSL 3.0 / TLS 1.0
9	0x0011	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA	SSL 3.0 / TLS 1.0
10	0x0012	TLS_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-DES-CBC-SHA	SSL 3.0 / TLS 1.0
11	0x0013	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA	SSL 3.0 / TLS 1.0
12	0x0014	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA	SSL 3.0 / TLS 1.0
13	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA	SSL 3.0 / TLS 1.0
14	0x0016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	SSL 3.0 / TLS 1.0
15	0x001E	TLS_KRB5_WITH_DES_CBC_SHA	KRB5-DES-CBC-SHA	SSL 3.0 / TLS 1.0
16	0x001F	TLS_KRB5_WITH_3DES_EDE_CBC_SHA	KRB5-DES-CBC3-SHA	SSL 3.0 / TLS 1.0
17	0x0020	TLS_KRB5_WITH_RC4_128_SHA	KRB5-RC4-SHA	SSL 3.0 / TLS 1.0
18	0x0022	TLS_KRB5_WITH_DES_CBC_MD5	KRB5-DES-CBC-MD5	SSL 3.0 / TLS 1.0
19	0x0023	TLS_KRB5_WITH_3DES_EDE_CBC_MD5	KRB5-DES-CBC3-MD5	SSL 3.0 / TLS 1.0
20	0x0024	TLS_KRB5_WITH_RC4_128_MD5	KRB5-RC4-MD5	SSL 3.0 / TLS 1.0
21	0x0026	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA	EXP-KRB5-DES-CBC-SHA	SSL 3.0 / TLS 1.0
22	0x0027	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA	EXP-KRB5-RC2-CBC-SHA	SSL 3.0 / TLS 1.0
23	0x0028	TLS_KRB5_EXPORT_WITH_RC4_40_SHA	EXP-KRB5-RC4-SHA	SSL 3.0 / TLS 1.0
24	0x0029	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5	EXP-KRB5-DES-CBC-MD5	SSL 3.0 / TLS 1.0
25	0x002A	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5	EXP-KRB5-RC2-CBC-MD5	SSL 3.0 / TLS 1.0
26	0x002B	TLS_KRB5_EXPORT_WITH_RC4_40_MD5	EXP-KRB5-RC4-MD5	SSL 3.0 / TLS 1.0
27	0x002F	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	SSL 3.0 / TLS 1.0
28	0x0032	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE-DSS-AES128-SHA	SSL 3.0 / TLS 1.0
29	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	SSL 3.0 / TLS 1.0
30	0x0035	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	SSL 3.0 / TLS 1.0
31	0x0038	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE-DSS-AES256-SHA	SSL 3.0 / TLS 1.0
32	0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	SSL 3.0 / TLS 1.0
33	0x0041	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA	SSL 3.0 / TLS 1.0
34	0x0044	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	DHE-DSS-CAMELLIA128-SHA	SSL 3.0 / TLS 1.0
35	0x0045	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA	SSL 3.0 / TLS 1.0
36	0x0062	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	EXP1024-DES-CBC-SHA	SSL 3.0 / TLS 1.0
37	0x0063	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	EXP1024-DHE-DSS-DES-CBC-SHA	SSL 3.0 / TLS 1.0
38	0x0064	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	EXP1024-RC4-SHA	SSL 3.0 / TLS 1.0
39	0x0084	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA	SSL 3.0 / TLS 1.0
40	0x0087	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	DHE-DSS-CAMELLIA256-SHA	SSL 3.0 / TLS 1.0
41	0x0088	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA	SSL 3.0 / TLS 1.0
42	0x008A	TLS_PSK_WITH_RC4_128_SHA	PSK-RC4-SHA	SSL 3.0 / TLS 1.0
43	0x008B	TLS_PSK_WITH_3DES_EDE_CBC_SHA	PSK-3DES-EDE-CBC-SHA	SSL 3.0 / TLS 1.0
44	0x008C	TLS_PSK_WITH_AES_128_CBC_SHA	PSK-AES128-CBC-SHA	SSL 3.0 / TLS 1.0
45	0x008D	TLS_PSK_WITH_AES_256_CBC_SHA	PSK-AES256-CBC-SHA	SSL 3.0 / TLS 1.0
46	0x0096	TLS_RSA_WITH_SEED_CBC_SHA	SEED-SHA	SSL 3.0 / TLS 1.0
47	0x0099	TLS_DHE_DSS_WITH_SEED_CBC_SHA	DHE-DSS-SEED-SHA	SSL 3.0 / TLS 1.0
48	0x009A	TLS_DHE_RSA_WITH_SEED_CBC_SHA	DHE-RSA-SEED-SHA	SSL 3.0 / TLS 1.0
49	0xC002	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	ECDH-ECDSA-RC4-SHA	SSL 3.0 / TLS 1.0
50	0xC003	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDH-ECDSA-DES-CBC3-SHA	SSL 3.0 / TLS 1.0
51	0xC004	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH-ECDSA-AES128-SHA	SSL 3.0 / TLS 1.0
52	0xC005	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	ECDH-ECDSA-AES256-SHA	SSL 3.0 / TLS 1.0
53	0xC007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	SSL 3.0 / TLS 1.0
54	0xC008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	SSL 3.0 / TLS 1.0
55	0xC009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	SSL 3.0 / TLS 1.0
56	0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	SSL 3.0 / TLS 1.0
57	0xC00C	TLS_ECDH_RSA_WITH_RC4_128_SHA	ECDH-RSA-RC4-SHA	SSL 3.0 / TLS 1.0
58	0xC00D	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	ECDH-RSA-DES-CBC3-SHA	SSL 3.0 / TLS 1.0
59	0xC00E	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	ECDH-RSA-AES128-SHA	SSL 3.0 / TLS 1.0
60	0xC00F	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	ECDH-RSA-AES256-SHA	SSL 3.0 / TLS 1.0
61	0xC011	TLS_ECDHE_RSA_WITH_RC4_128_SHA	ECDHE-RSA-RC4-SHA	SSL 3.0 / TLS 1.0
62	0xC012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	SSL 3.0 / TLS 1.0
63	0xC013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	SSL 3.0 / TLS 1.0
64	0xC014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	SSL 3.0 / TLS 1.0
65	0x010080	SSL_CK_RC4_128_WITH_MD5	RC4-MD5	SSL 2.0
66	0x020080	SSL_CK_RC4_128_EXPORT40_WITH_MD5	EXP-RC4-MD5	SSL 2.0
67	0x030080	SSL_CK_RC2_128_CBC_WITH_MD5	RC2-CBC-MD5	SSL 2.0
68	0x040080	SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	EXP-RC2-CBC-MD5	SSL 2.0
69	0x050080	SSL_CK_IDEA_128_CBC_WITH_MD5	IDEA-CBC-MD5	SSL 2.0
70	0x060040	SSL_CK_DES_64_CBC_WITH_MD5	DES-CBC-MD5	SSL 2.0
71	0x0700C0	SSL_CK_DES_192_EDE3_CBC_WITH_MD5	DES-CBC3-MD5	SSL 2.0

図表：利用可能な Cipher suite

また、調査結果から以下のような傾向があった。

- OpenSSL0.9.8e 及び OpenSSL0.9.8r のデフォルト設定では、SSL2.0 の推奨されていない暗号アルゴリズムを含んだ Cipher suite が利用可能であるが、OpenSSL1.0.0 e のデフ

ォルト設定では、SSL2.0 の推奨されていない暗号アルゴリズムを含んだ Cipher suite が利用不可な設定に変更されている。

- OpenSSL0.9.8r のデフォルト設定では、各 OS における差異は殆ど無いが、OpenSSL1.0.0 e では RHEL5.4 のみ設定が異なる。
  なお、RHEL は 5.4 では OpenSSL0.9.8e 及び OpenSSL0.9.8、6.1 では OpenSSL1.0.0 e をパッケージとしてサポートしており、独自に設定された OpenSSL がデフォルトで組み込まれている。そのため、OpenSSL を個別インストールしたものとは設定が異なる。
  具体的には、Kerberos のサポート及び ECDH 系鍵交換プロトコルの非サポートである。
- IIS6.0、IIS7.0、IIS7.5 のデフォルト設定では、SSL2.0 の推奨されていない暗号アルゴリズムを含んだ Cipher suite が利用可能である。
- IIS6.0 のデフォルト設定では、推奨されていない暗号アルゴリズムを含んだ Cipher suite だけが利用可能であり、推奨されている暗号アルゴリズムのみで構成された Cipher suite は個別に利用可能な設定に変更する必要がある。

なお、調査した各サーバ系環境での対比など詳細な結果については、付録１を参照。

3.2.2 クライアント系設定調査結果

各クライアント環境において利用可能な Cipher suite 数の調査結果を以下に示す。なお、詳細結果については、付録２を参照。

ブラウザ	OS	利用可能な Cipher suite数
Internet Explorer 7	Windows XP	11
	Windows Vista	12
Internet Explorer 8	Windows XP	11
	Windows Vista	12
	Windows 7 Home	12
	Windows 7 Professiona	12
Internet Explorer 9	Windows Vista	12
	Windows 7 Home	12
	Windows 7 Professiona	12
Safari 5	Windows XP	11
	Windows Vista	12
	Windows 7 Home	12
	Windows 7 Professiona	12
	MacOS X	27
Opera 11.50	Windows XP	27
	Windows Vista	28
	Windows 7 Home	27
	Windows 7 Professiona	27
	MacOS X	28
	Ubuntu 11.10 Desktop	28

ブラウザ	OS	利用可能な Cipher suite数
Firefox 3.6	Windows XP	36
	Windows Vista	36
	Windows 7 Home	36
	Windows 7 Professional	36
	MacOS X	36
	Ubuntu 11.10 Desktop	36
Firefox 7	Windows XP	36
	Windows Vista	36
	Windows 7 Home	36
	Windows 7 Professional	36
	MacOS X	36
	Ubuntu 11.10 Desktop	36
Google Chrome 12	Windows XP	36
	Windows Vista	36
	Windows 7 Home	36
	Windows 7 Professional	36
	MacOS X	36
	Ubuntu 11.10 Desktop	36

図表：クライアント環境設定における利用可能な Cipher suite 数

次に、各クライアント環境のデフォルト設定時の Cipher suite の優先順位の調査結果を以下に示す。なお、下表で Cipher suite を示した行は、各クライアント環境に合わせて表記しているため、各クライアント環境によって異なる。すべてのクライアント環境を横並びに確認する場合は、付録２を参照。

(1) Internet Explore のデフォルト設定時の Cipher suite 優先順位の結果

Internet Explore の Cipher suite 優先順位（デフォルト設定時）の結果として特出すべき点は、Windows XP は、他の OS に比べ、推奨されていない Cipher suite が選択されている傾向にある。これは、Windows Vista や Windows 7 に比べ、開発・発売期間が古いことが原因と考えられるが、この設定（Cipher suite の選択）は、Internet Explore8 の環境においても変わらないため、新規のブラウザを利用することで推奨されている Cipher suite を選択するように改善される結果に至っていない。

Cipher Suite		Internet Explorer (IE7)		Internet Explorer (IE8)				Internet Explorer (IE9)		
No.	Cipher Suite	Windows XP	Windows Vista	Windows XP	Windows Vista	Windows 7 Home	Windows 7 Pro	Windows Vista	Windows 7 Home	Windows 7 Pro
CS1	TLS_RSA_EXPORT_WITH_RC4_40_MD5	7		7						
CS2	TLS_RSA_WITH_RC4_128_MD5	1	12	1	12	12	12	12	12	12
CS3	TLS_RSA_WITH_RC4_128_SHA	2	3	2	3	3	3	3	3	3
CS4	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	8		8						
CS5	TLS_RSA_WITH_DES_CBC_SHA	4		4						
CS6	TLS_RSA_WITH_3DES_EDE_CBC_SHA	3	4	3	4	4	4	4	4	4
CS9	TLS_DHE_DSS_WITH_DES_CBC_SHA	10		10						
CS10	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	9	11	9	11	11	11	11	11	11
CS12	TLS_RSA_WITH_AES_128_CBC_SHA		1		1	1	1	1	1	1
CS15	TLS_DHE_DSS_WITH_AES_128_CBC_SHA		9		9	9	9	9	9	9
CS17	TLS_RSA_WITH_AES_256_CBC_SHA		2		2	2	2	2	2	2
CS20	TLS_DHE_DSS_WITH_AES_256_CBC_SHA		10		10	10	10	10	10	10
CS30	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	6		6						
CS31	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	11		11						
CS32	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	5		5						
CS49	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		5		5	7	7	5	7	7
CS50	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		6		6	8	8	6	8	8
CS57	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		7		7	5	5	7	5	5
CS58	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		8		8	6	6	8	6	6

図表： Internet Explore の Cipher suite の優先順位

(2) Firefox のデフォルト設定時の Cipher suite 優先順位の結果

Firefox の Cipher suite 優先順位（デフォルト設定時）の結果として特出すべき点は、バージョンを問わず、すべての Cipher suite の選択が変わらないことである。また、Firefox で選択可能な Cipher suite が他のブラウザに比べ多い傾向にある。

Cipher Suite		Firefox (Firefox 3.6)						Firefox (Firefox 7)					
No.	Cipher Suite	Windows XP	Windows Vista	Windows 7 Home	Windows 7 Pro	Mac OS X	Ubuntu 11.10 D	Windows XP	Windows Vista	Windows 7 Home	Windows 7 Pro	Mac OS X	Ubuntu 11.10 D
CS2	TLS_RSA_WITH_RC4_128_MD5	25	25	25	25	25	25	25	25	25	25	25	25
CS3	TLS_RSA_WITH_RC4_128_SHA	26	26	26	26	26	26	26	26	26	26	26	26
CS6	TLS_RSA_WITH_3DES_EDE_CBC_SHA	35	35	35	35	35	35	35	35	35	35	35	35
CS10	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	31	31	31	31	31	31	31	31	31	31	31	31
CS11	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	30	30	30	30	30	30	30	30	30	30	30	30
CS12	TLS_RSA_WITH_AES_128_CBC_SHA	27	27	27	27	27	27	27	27	27	27	27	27
CS15	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	18	18	18	18	18	18	18	18	18	18	18	18
CS16	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	17	17	17	17	17	17	17	17	17	17	17	17
CS17	TLS_RSA_WITH_AES_256_CBC_SHA	9	9	9	9	9	9	10	10	10	10	10	10
CS20	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	5	5	5	5	5	5	6	6	6	6	6	6
CS21	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	10	10	10	10	10	10	5	5	5	5	5	5
CS27	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	24	24	24	24	24	24	24	24	24	24	24	24
CS28	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	16	16	16	16	16	16	16	16	16	16	16	16
CS29	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	15	15	15	15	15	15	15	15	15	15	15	15
CS39	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	8	8	8	8	8	8	9	9	9	9	9	9
CS40	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	4	4	4	4	4	4	4	4	4	4	4	4
CS41	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	3	3	3	3	3	3	3	3	3	3	3	3
CS42	TLS_RSA_WITH_SEED_CBC_SHA	23	23	23	23	23	23	23	23	23	23	23	23
CS43	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	21	21	21	21	21	21	21	21	21	21	21	21
CS44	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	33	33	33	33	33	33	33	33	33	33	33	33
CS45	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	22	22	22	22	22	22	22	22	22	22	22	22
CS46	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	7	7	7	7	7	7	8	8	8	8	8	8
CS47	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	11	11	11	11	11	11	11	11	11	11	11	11
CS48	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	28	28	28	28	28	28	28	28	28	28	28	28
CS49	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	12	12	12	12	12	12	12	12	12	12	12	12
CS50	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	1	1	1	1	1	1	1	1	1	1	1	1
CS51	TLS_ECDH_RSA_WITH_RC4_128_SHA	19	19	19	19	19	19	19	19	19	19	19	19
CS52	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	32	32	32	32	32	32	32	32	32	32	32	32
CS53	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	20	20	20	20	20	20	20	20	20	20	20	20
CS54	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	6	6	6	6	6	6	7	7	7	7	7	7
CS55	TLS_ECDHE_RSA_WITH_RC4_128_SHA	13	13	13	13	13	13	13	13	13	13	13	13
CS56	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	29	29	29	29	29	29	29	29	29	29	29	29
CS57	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	14	14	14	14	14	14	14	14	14	14	14	14
CS58	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	2	2	2	2	2	2	2	2	2	2	2	2
CS59	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	34	34	34	34	34	34	34	34	34	34	34	34

図表： Firefox の Cipher suite の優先順位

(3) Opera のデフォルト設定時の Cipher suite 優先順位の結果

Opera の Cipher suite 優先順位（デフォルト設定時）の結果として特出すべき点は、バージョンを問わず、すべての Cipher suite の選択が変わらないことである。

Cipher Suite		Opera (Opera 11.52)					
No.	Cipher Suite	Windows XP	Windows Vista	Windows 7 Home	Windows 7 Pro	Mac OS X	Ubuntu 11.10 D
CS2	TLS_RSA_WITH_RC4_128_MD5	22	22	22	22	22	22
CS3	TLS_RSA_WITH_RC4_128_SHA	21	21	21	21	21	21
CS6	TLS_RSA_WITH_3DES_EDE_CBC_SHA	27	27	27	27	27	27
CS7	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	24	24	24	24	24	24
CS8	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	26	26	26	26	26	26
CS10	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	23	23	23	23	23	23
CS11	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	25	25	25	25	25	25
CS12	TLS_RSA_WITH_AES_128_CBC_SHA	20	20	20	20	20	20
CS13	TLS_DH_DSS_WITH_AES_128_CBC_SHA	19	19	19	19	19	19
CS14	TLS_DH_RSA_WITH_AES_128_CBC_SHA	18	18	18	18	18	18
CS15	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	17	17	17	17	17	17
CS16	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	16	16	16	16	16	16
CS17	TLS_RSA_WITH_AES_256_CBC_SHA	10	10	10	10	10	10
CS18	TLS_DH_DSS_WITH_AES_256_CBC_SHA	9	9	9	9	9	9
CS19	TLS_DH_RSA_WITH_AES_256_CBC_SHA	8	8	8	8	8	8
CS20	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	7	7	7	7	7	7
CS21	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	6	6	6	6	6	6
CS22	TLS_RSA_WITH_AES_128_CBC_SHA256	15	15	15	15	15	15
CS23	TLS_RSA_WITH_AES_256_CBC_SHA256	5	5	5	5	5	5
CS24	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	14	14	14	14	14	14
CS25	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	13	13	13	13	13	13
CS26	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	12	12	12	12	12	12
CS33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	11	11	11	11	11	11
CS34	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	4	4	4	4	4	4
CS35	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	3	3	3	3	3	3
CS37	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	2	2	2	2	2	2
CS38	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	1	1	1	1	1	1

図表： Opera の Cipher suite の優先順位

(4) Google Chrome のデフォルト設定時の Cipher suite 優先順位の結果

Google Chrome の Cipher suite 優先順位（デフォルト設定時）の結果として特出すべき点は、バージョンを問わず、すべての Cipher suite の選択が変わらないことである。

なお、Google Chrome の結果については、Safari の結果の表に含める。

(5) Safari のデフォルト設定時の Cipher suite 優先順位の結果

Safari の Cipher suite 優先順位（デフォルト設定時）の結果として特出すべき点は、他のブラウザの設定や OS の設定を参照して Cipher suite が選択される傾向にある。例えば、Windows XP では、Windows XP の Internet Explorer7 や Internet Explorer8 とまったく同一であり、Windows Vista や Windows 7 では、Internet Explorer7、8、9 とまったく同一である。

Cipher Suite		Google Chrome (Chrome 15)						Safari (Safari 5.1.1)				
No.	Cipher Suite	Windows XP	Windows Vista	Windows 7 Home	Windows 7 Pro	Mac OS X	Ubuntu 11.10 D	Windows XP	Windows Vista	Windows 7 Home	Windows 7 Pro	Mac OS X
CS1	TLS_RSA_EXPORT_WITH_RC4_40_MD5							7				
CS2	TLS_RSA_WITH_RC4_128_MD5	26	26	26	26	26	26	1	12	12	12	19
CS3	TLS_RSA_WITH_RC4_128_SHA	27	27	27	27	27	27	2	3	3	3	18
CS4	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5							8				
CS5	TLS_RSA_WITH_DES_CBC_SHA							4				
CS6	TLS_RSA_WITH_3DES_EDE_CBC_SHA	36	36	36	36	36	36	3	4	4	4	21
CS9	TLS_DHE_DSS_WITH_DES_CBC_SHA							10				
CS10	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	32	32	32	32	32	32	9	11	11	11	27
CS11	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	31	31	31	31	31	31					26
CS12	TLS_RSA_WITH_AES_128_CBC_SHA	28	28	28	28	28	28		1	1	1	17
CS15	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	19	19	19	19	19	19		9	9	9	22
CS16	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	18	18	18	18	18	18					23
CS17	TLS_RSA_WITH_AES_256_CBC_SHA	10	10	10	10	10	10		2	2	2	20
CS20	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	6	6	6	6	6	6		10	10	10	24
CS21	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	5	5	5	5	5	5					25
CS27	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	25	25	25	25	25	25					
CS28	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	16	16	16	16	16	16					
CS29	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	15	15	15	15	15	15					
CS30	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA							6				
CS31	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA							11				
CS32	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA							5				
CS36	TLS_DHE_DSS_WITH_RC4_128_SHA	17	17	17	17	17	17					
CS39	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9	9	9	9	9	9					
CS40	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	4	4	4	4	4	4					
CS41	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	3	3	3	3	3	3					
CS42	TLS_RSA_WITH_SEED_CBC_SHA	24	24	24	24	24	24					
CS43	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	22	22	22	22	22	22					11
CS44	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	34	34	34	34	34	34					12
CS45	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	23	23	23	23	23	23					9
CS46	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	8	8	8	8	8	8					10
CS47	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	11	11	11	11	11	11					3
CS48	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	29	29	29	29	29	29					4
CS49	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	12	12	12	12	12	12		5	7	7	2
CS50	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	1	1	1	1	1	1		6	8	8	1
CS51	TLS_ECDH_RSA_WITH_RC4_128_SHA	20	20	20	20	20	20					15
CS52	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	33	33	33	33	33	33					16
CS53	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	21	21	21	21	21	21					13
CS54	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	7	7	7	7	7	7					14
CS55	TLS_ECDHE_RSA_WITH_RC4_128_SHA	13	13	13	13	13	13					7
CS56	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	30	30	30	30	30	30					8
CS57	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	14	14	14	14	14	14		7	5	5	5
CS58	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	2	2	2	2	2	2		8	6	6	6
CS59	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	35	35	35	35	35	35					

図表：Google Chrome／Safari **の** Cipher suite **の優先順位**

3.3 ＳＳＬサーバ設定調査結果

本節では、２.３節から２.５節で示した調査対象となる SSL サーバに対する調査結果を報告する。

3.3.1 Cipher suite の通信可否調査結果

本小節では、３.２.１の結果を基に、各種のサーバ系環境で利用可能な Cipher suite について、調査対象 SSL サーバに対して通信可否の調査を行った結果を報告する。

この調査は、２.３節の（１）で示した通り、各種ブラウザの影響を受けない方法で調査した結果である。各業界別の調査結果を以下に示す。下表では、通信可能であった Cipher suite が少なくとも 1 つ以上あったものを●印で示す。本調査で確認された Cipher suite は、27 種類であり、そのうち、推奨されている共通鍵暗号アルゴリズム及びメッセージ認証は、8 種類ある。（下表では、黄色枠の Cipher suite である。）

	CS-No	Cipher suite	金融系	物販系	非物販系
1	CS1	EXP-RC4-MD5	●	●	●
2	CS2	RC4-MD5	●	●	●
3	CS3	RC4-SHA	●	●	●
4	CS4	EXP-RC2-CBC-MD5	●	●	●
5	CS5	IDEA-CBC-SHA	●	●	●
6	CS6	EXP-DES-CBC-SHA	●	●	●
7	CS7	DES-CBC-SHA	●	●	●
8	CS8	DES-CBC3-SHA	●	●	●
9	CS12	EXP-EDH-RSA-DES-CBC-SHA	●	●	●
10	CS13	EDH-RSA-DES-CBC-SHA	●	●	●
11	CS14	EDH-RSA-DES-CBC3-SHA	●	●	●
12	CS27	AES128-SHA	●	●	●
13	CS29	DHE-RSA-AES128-SHA	●	●	●
14	CS30	AES256-SHA	●	●	●
15	CS32	DHE-RSA-AES256-SHA	●	●	●
16	CS33	CAMELLIA128-SHA	―	●	―
17	CS36	EXP1024-DES-CBC-SHA	●	●	●
18	CS38	EXP1024-RC4-SHA	●	●	●
19	CS39	CAMELLIA256-SHA	―	●	―
20	CS46	SEED-SHA	―	●	―
21	CS63	ECDHE-RSA-AES128-SHA	―	●	●
22	CS64	ECDHE-RSA-AES256-SHA	―	●	●
23	CS65	RC4-MD5	●	●	●
24	CS66	EXP-RC4-MD5	●	●	●
25	CS69	IDEA-CBC-MD5	―	●	●
26	CS70	DES-CBC-MD5	●	●	●
27	CS71	DES-CBC3-MD5	●	●	●

図表：調査対象３業界で利用可能な Cipher suite（ブラウザ未使用）

金融系は、利用可能な Cipher suite が 21 種類であり、そのうち上記の推奨された共通鍵暗号アルゴリズム及びメッセージ認証を利用できる Cipher suite は 4 種類である。また、CS39～CS64 等が利用できない設定であり、3 業界中で最も利用可能な Cipher suite が限定されている。

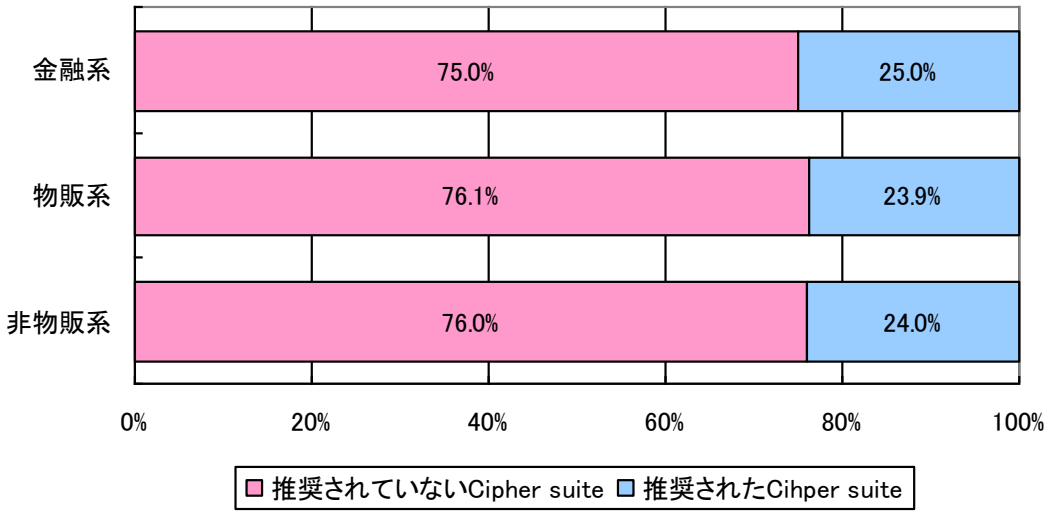
物販系は、利用可能な Cipher suite が 27 種類であり、そのうち上記の推奨された共通鍵暗号ア

ルゴリズム及びメッセージ認証を利用できる Cipher suite は 8 種類であり、物販系は、SSL3.0/TLS1.0 及び SSL2.0 を含むすべての Cipher suite で通信が可能であった。

非物販系は、利用可能な Cipher suite が 24 種類であり、そのうち上記の推奨された共通鍵暗号アルゴリズム及びメッセージ認証を利用できる Cipher suite は 6 種類である。また、非物販系は、金融系との比較において、CS63 や CS64 が利用可能であり、Cipher suite の限定としては、3 業界の中で中程度であった。

また、上記で調査した各種の Cipher suite について、①推奨された暗号アルゴリズムのみで構成された Cipher suite（以下、推奨された Cipher suite と略す）と、②推奨されていない暗号アルゴリズムを含んだ Cipher suite（以下、推奨されていない Cipher suite と略す）の利用について以下に報告する。

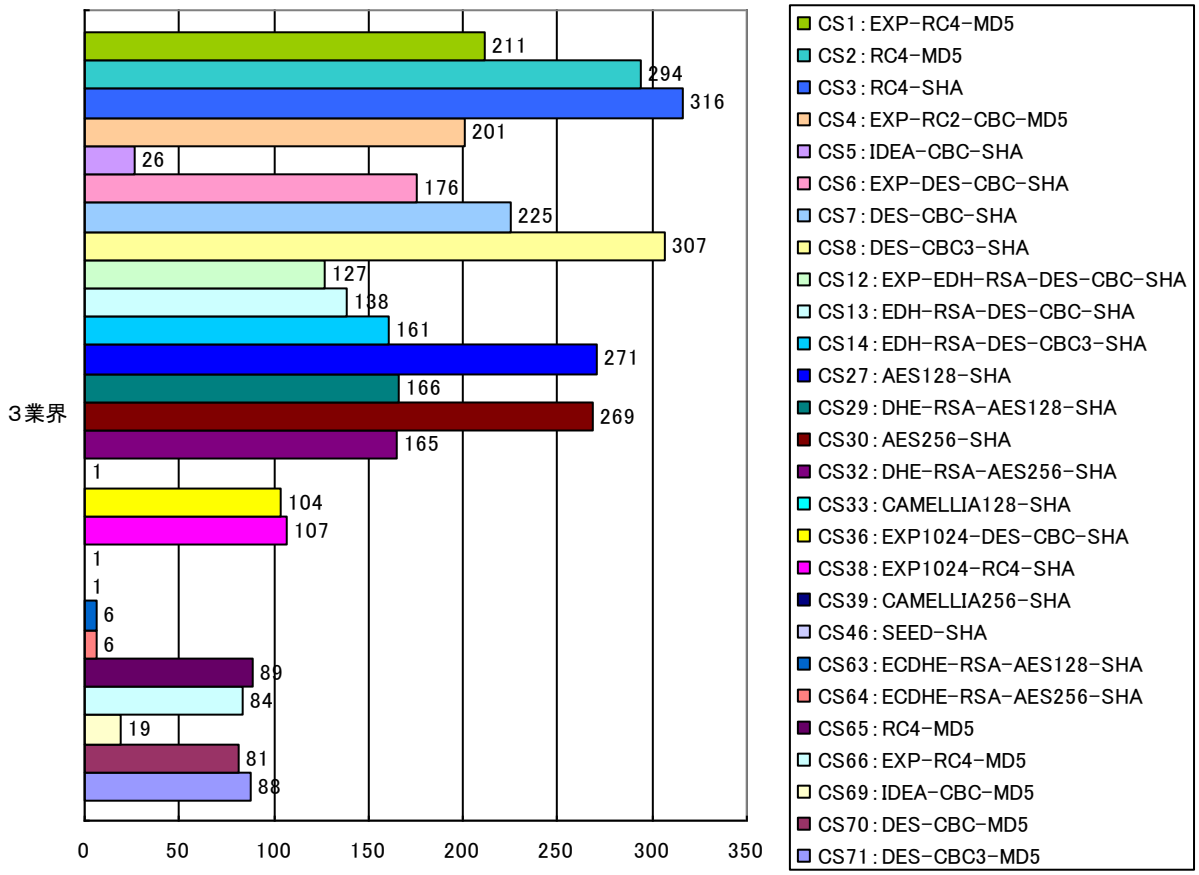
金融系、物販系、非物販系で利用可能な Cipher suite の率は、以下の通りである。②推奨されていない Cipher suite の率は、物販系、非物販系が 76%とほぼ同数であり、次いで金融系が 75%であった。3 業界の結果はとして、①推奨された Cipher suite の利用可能な率は 30%以下と、総じて低い結果であった。



図表：調査対象３業界で利用可能な推奨された Cipher suite の率（ブラウザ未使用）＜対象サーバ：324＞

3.3.2　業界別の調査結果

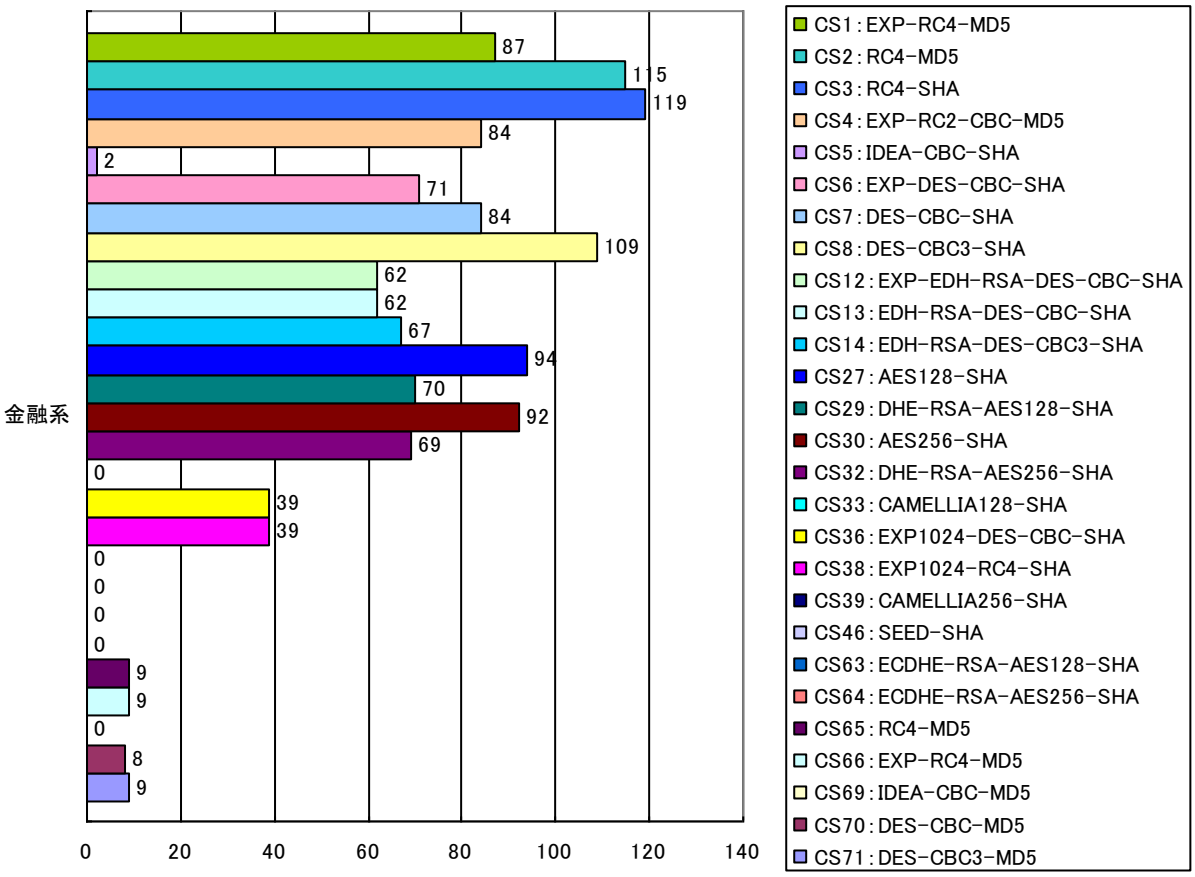
本調査の３業界を合算した結果を以下に報告する。３業界合計で利用可能な暗号アルゴリズムの上位５種類については、上位から RC4-SHA が 316、DES-CBC3-SHA が 307、RC4-MD5 が 294、AES128-SHA が 271、AES265-SHA が 269 という結果であった。



図表：調査対象（３業界合計）で接続に利用した Cipher suite**（ブラウザ未使用）<対象サーバ：**324>

(1) **金融系について**

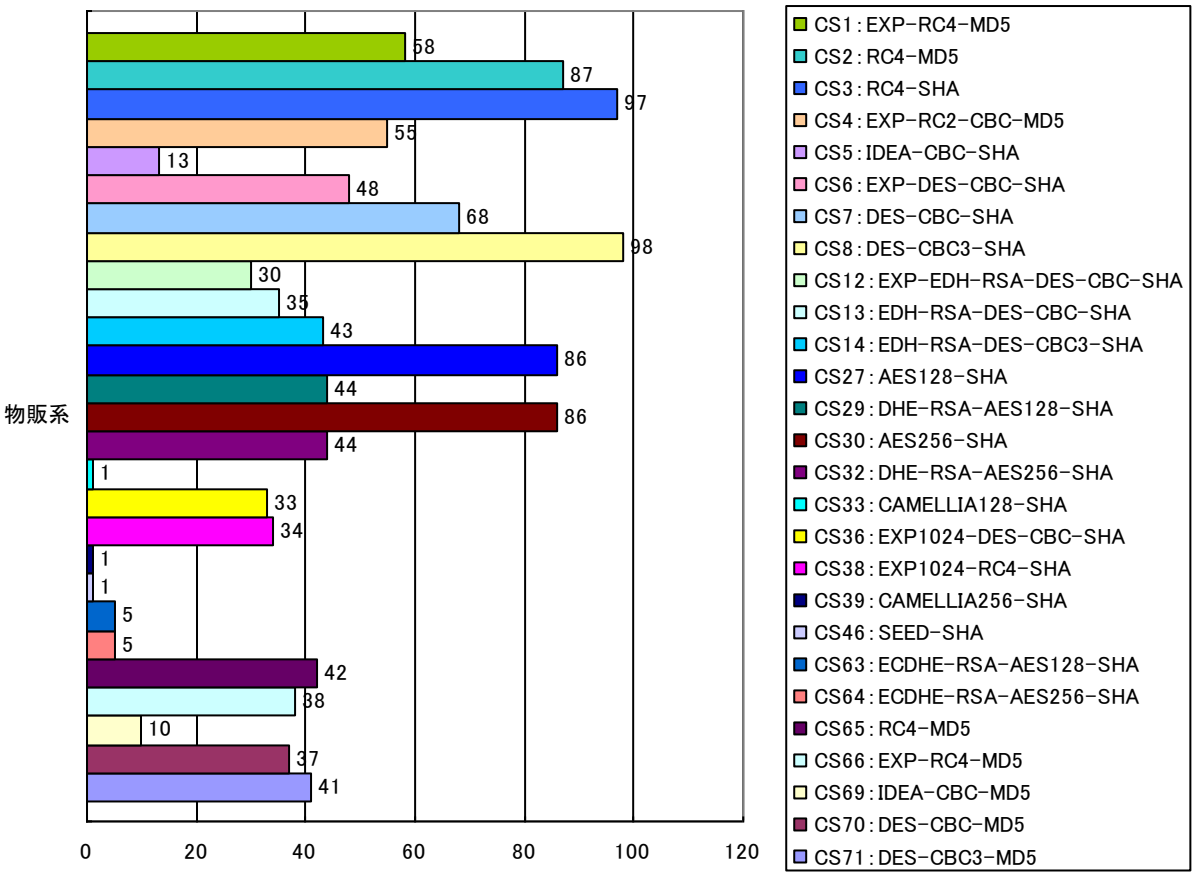
金融系で利用が可能な暗号アルゴリズムの上位 5 種類については、上位から RC4-SHA **が** 119、RC4-MD5 **が** 115、DES-CBC3-SHA **が** 109、AES128-SHA **が** 94、AES265-SHA **が** 92 **という結果であった。**



図表：調査対象（金融系）で接続に利用した Cipher suite**（ブラウザ未使用）<対象サーバ：**122>

⑵ **物販系について**

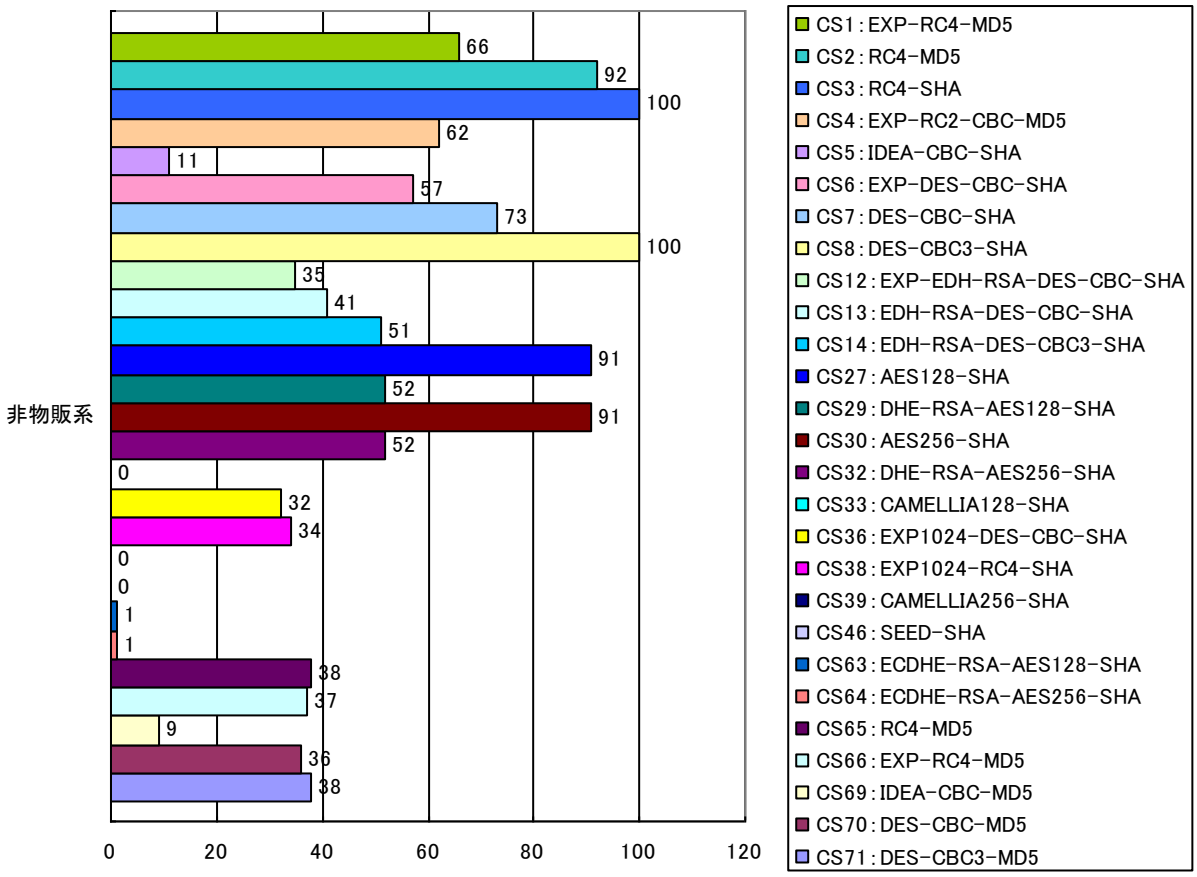
物販系で利用が可能な暗号アルゴリズムの上位 5 種類については、上位から DES-CBC3-SHA **が** 98、RC4-SHA **が** 97、RC4-MD5 **が** 87、AES128-SHA **と** AES265-SHA **がともに** 86 **という結果であった。**



図表：調査対象（物販系）で接続に利用した Cipher suite**（ブラウザ未使用）<対象サーバ：**100>

(3) **非物販系について**

非物販系で利用が可能な暗号アルゴリズムの上位 5 種類については、上位から RC4-SHA **と** DES-CBC3-SHA **がともに** 100**、**RC4-MD5 **が** 92**、**AES128-SHA **と** AES265-SHA **がともに** 91 **という結果であった。**



図表：調査対象（非物販系）で接続に利用した Cipher suite**（ブラウザ未使用）<対象サーバ：**102>

3.3.3 クライアント環境における Cipher suite 調査結果

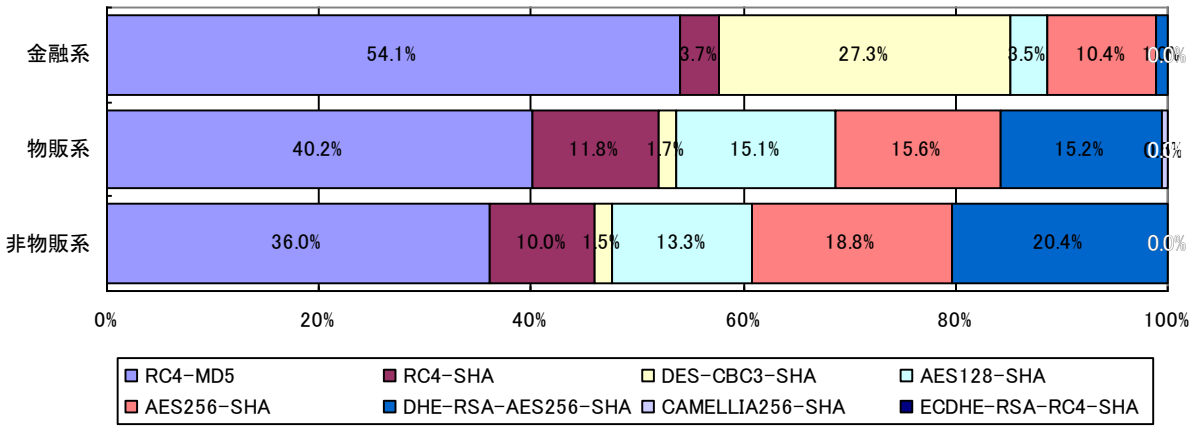
本調査結果は、２.３節の（２）で示した通り、2.3.1 **に示したクライアント環境を用いて調査した結果である。各業界別の調査結果を以下に示す。下表では、通信可能であった** Cipher suite **が少なくとも** 1 **つ以上あったものを●印で示す。本調査で確認された** Cipher suite **は、**8 **種類であり、そのうち、推奨されている共通鍵暗号アルゴリズム及びメッセージ認証は、**4 **種類ある。（下表では、黄色枠の** Cipher suite **である。）**

	CS-No	Cipher suite	金融系	物販系	非物販系
1	CS2	TLS_RSA_WITH_RC4_128_MD5	●	●	●
2	CS3	TLS_RSA_WITH_RC4_128_SHA	●	●	●
3	CS8	TLS_RSA_WITH_3DES_EDE_CBC_SHA	●	●	●
4	CS27	TLS_RSA_WITH_AES_128_CBC_SHA	●	●	●
5	CS30	TLS_RSA_WITH_AES_256_CBC_SHA	●	●	●
6	CS32	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	●	●	●
7	CS39	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	―	●	―
8	CS61	TLS_ECDHE_RSA_WITH_RC4_128_SHA	●	―	―

図表：調査対象３業界において接続に利用した Cipher suite**（各種ブラウザ使用）**

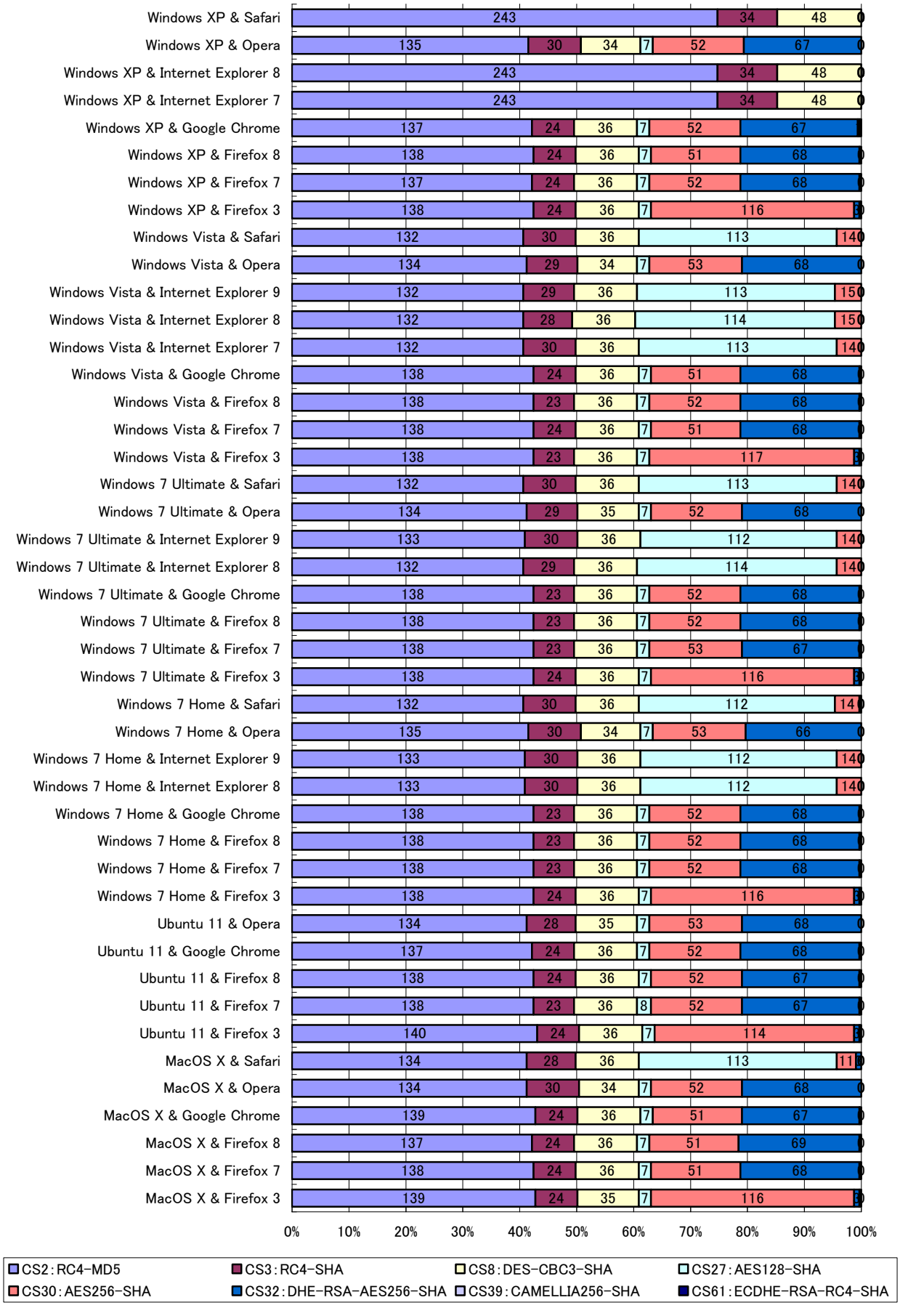
各業界の傾向を以下に示す。下表では、推奨されていない共通鍵暗号アルゴリズム及びメッセージ認証と推奨されている共通鍵暗号アルゴリズム及びメッセージ認証を記している。推奨されていない共通鍵暗号アルゴリズム及びメッセージ認証は、[CS2]RC4-MD5（下表では紫色）、[CS3]RC4-SHA（下表では赤紫色）、[CS8]3DES-SHA（下表では白乳色）等であり、本調査結果の大半を占める。推奨されている共通鍵暗号アルゴリズム及びメッセージ認証は、[CS27]AES128-SHA（下表では淡青色）、[CS29]AES128-SHA（下表では桃色）、[CS32]AES256-SHA（下表では青色）等であり、上記の Cipher suite に次いで多い結果である。
（以降、本調査報告書では、同じ配色でグラフ化しているため、推奨されていない共通鍵暗号アルゴリズム及びメッセージ認証で構成された Cipher suite と、推奨されている共通鍵暗号アルゴリズム及びメッセージ認証で構成された Cipher suite について分析を行う。）

下表で示した通り、金融系では、約 80%以上が推奨されていない Cipher suite によって接続し、3 業界の中で最も利用率が高い。続いて、物販系が約 55%程度、非物販系が約 50%程度であった。金融系の SSL サーバに対する Cipher suite の調査は、2008 年、2009 年と実施[1] [2] [9] [10]されていたが、調査対象となる SSL サーバが、本調査結果と異なることも考えられ、本調査結果との単純比較や推移を求められない。

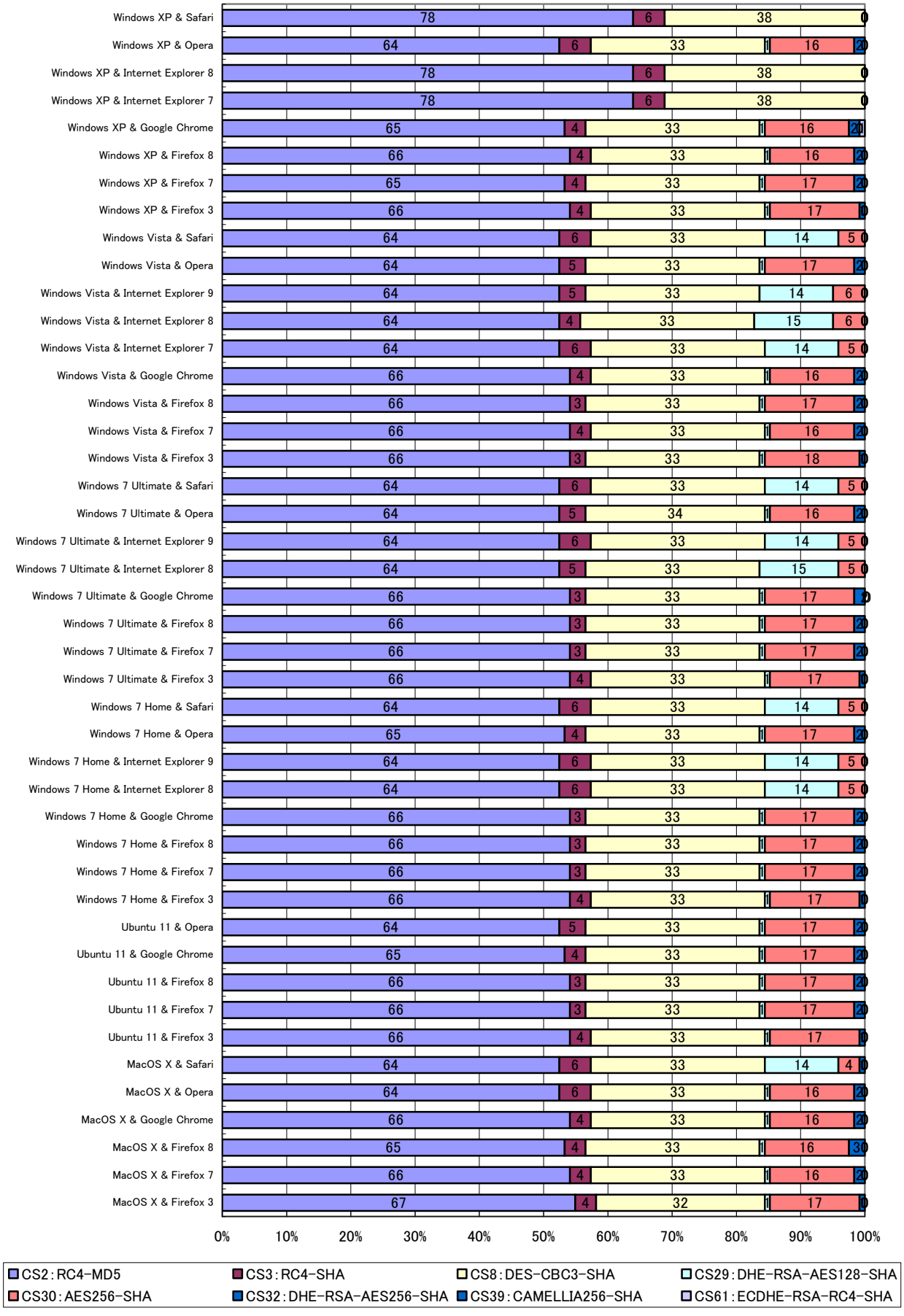


図表：調査対象３業界において接続に利用した Cipher suite　<対象サーバ：325>

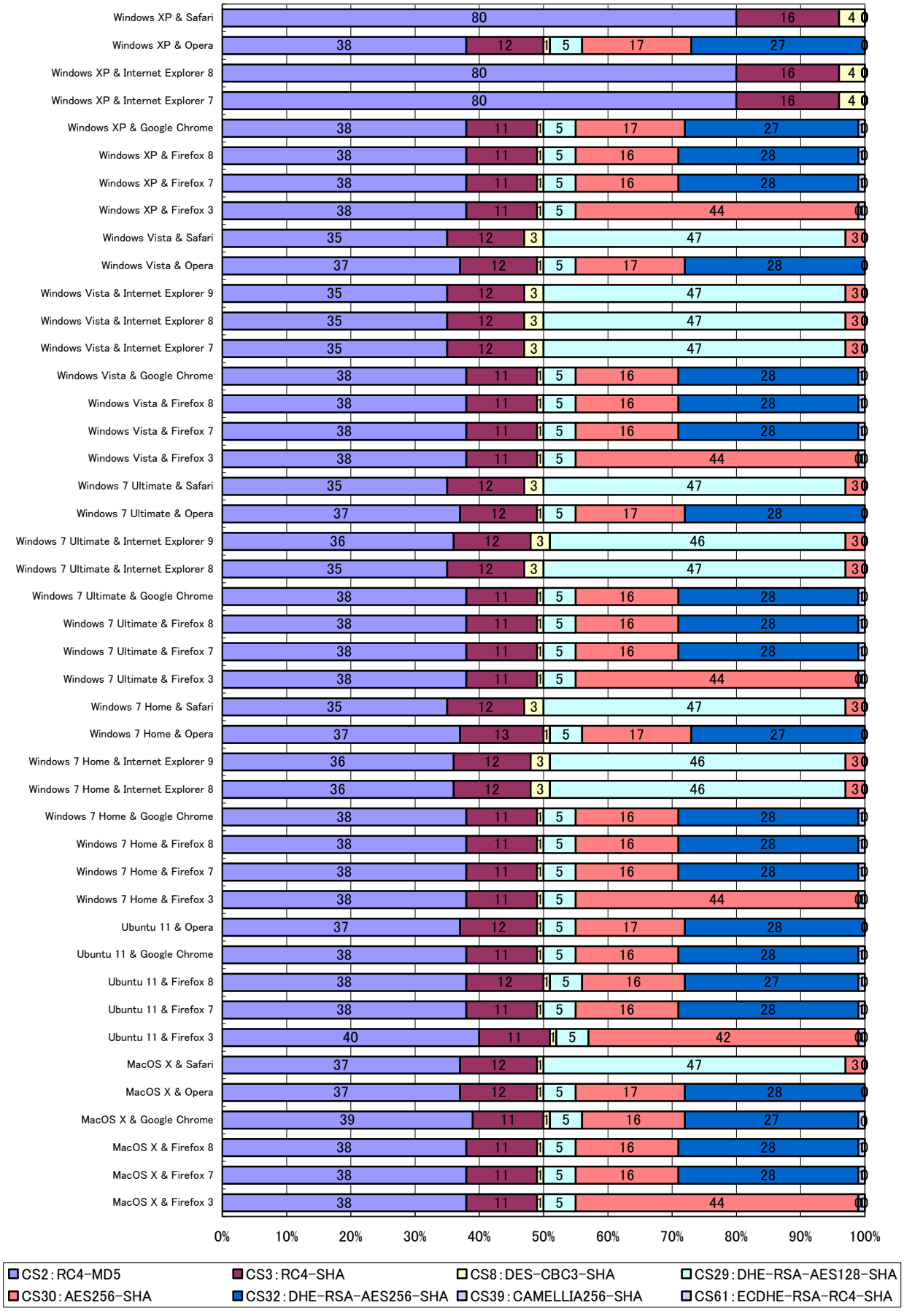
また、個別のクライアント環境における調査結果を以下に示す。



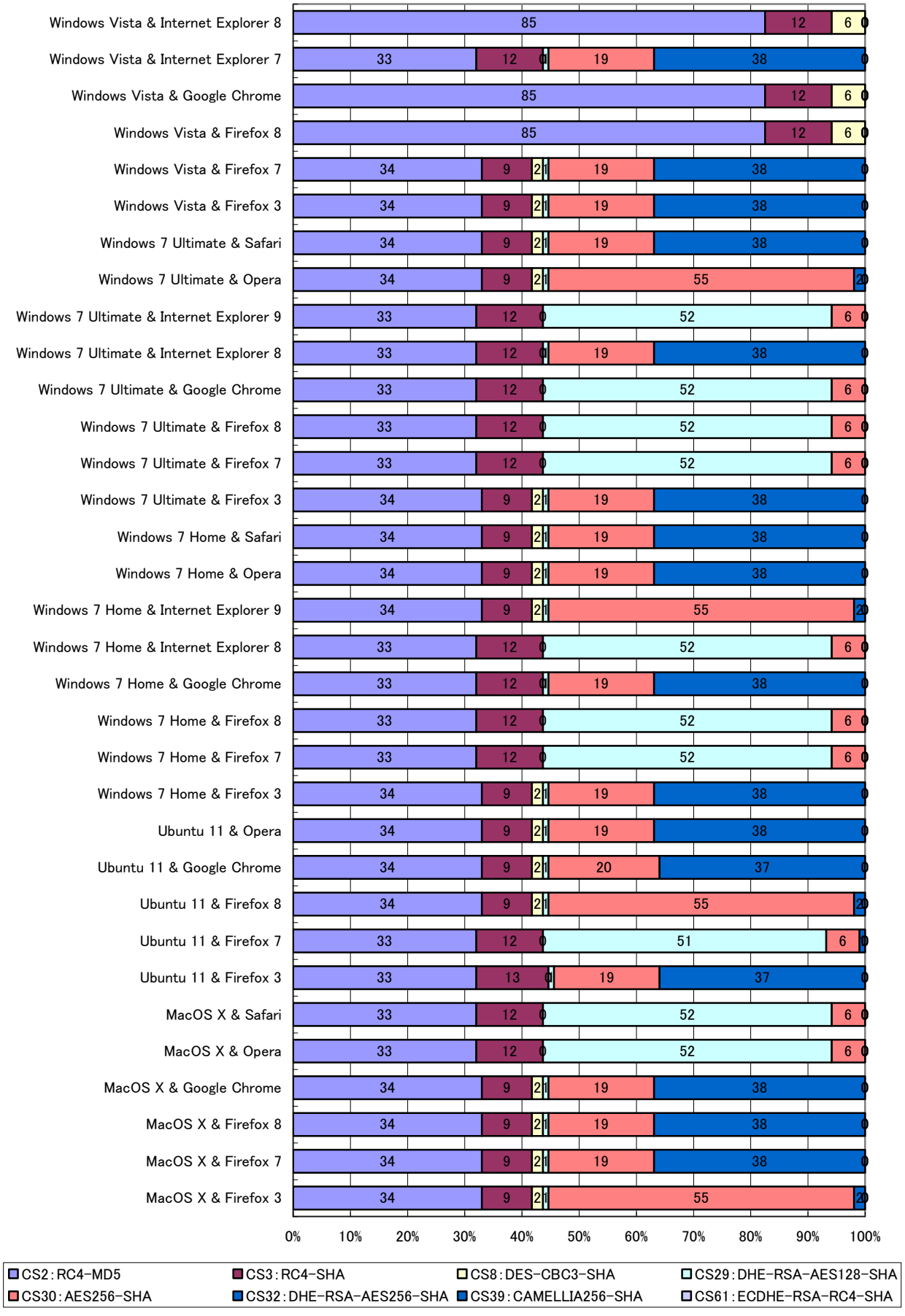
図表：各クライアント環境において利用した Cipher suite の詳細（３業界合計／ブラウザ使用）
<対象サーバ：325>



図表：各クライアント環境において利用した Cipher suite の詳細（金融系／ブラウザ使用）
<対象サーバ：122>



図表：各クライアント環境において利用した Cipher suite の詳細（物販系／ブラウザ使用）
<対象サーバ：100>



図表：各クライアント環境において利用した Cipher suite の詳細（非物販系／ブラウザ使用）
<対象サーバ：103>

3.3.4　各ＯＳにおける調査結果

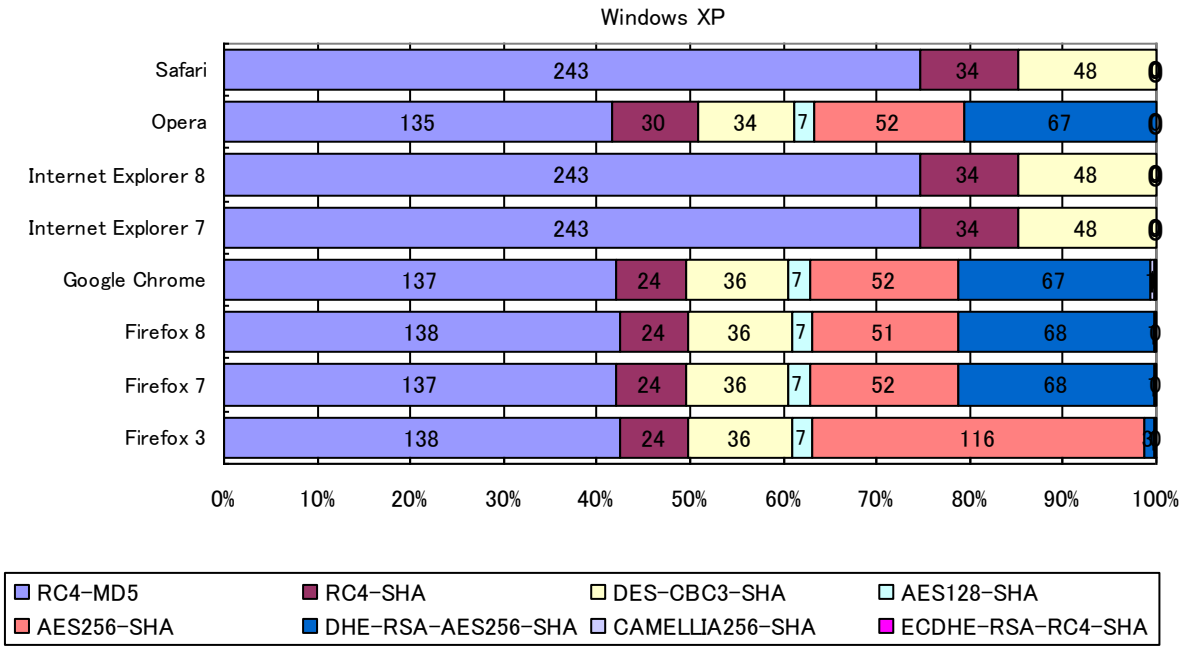
調査結果について、調査分析（２）の観点から、各ＯＳを軸として整理・分析した結果を以下に示す。

(1) Windows XP 環境について

Windows XP 環境において、推奨されていない Cipher suite を使って接続する率は、他の OS に比べて高く、特に Internet Explorer8、Safari、Internet Explorer7 は 100%であり、その他のブラウザは、約 60%であった。

また、Windows XP 環境おいて利用されている Cipher suite については、OS と各ブラウザ間での有意な相関性は認められなかった。

但し、Internet Explorer のバージョンアップ（下表 Internet Explorer7 と Internet Explorer8）、及び Firefox のバージョンアップ(下表 Firefox3 から Firefox7 や Firefox8 へのバージョンアップ）による Cipher suite の利用選択については、必ずしも推奨された暗号アルゴリズムが選択される傾向（例えば、DES から AES へ選択が移行される傾向）ではない結果となっている点に注意する必要がある。



図表：Windows XP で接続に利用した Cipher suite <対象サーバ：325>

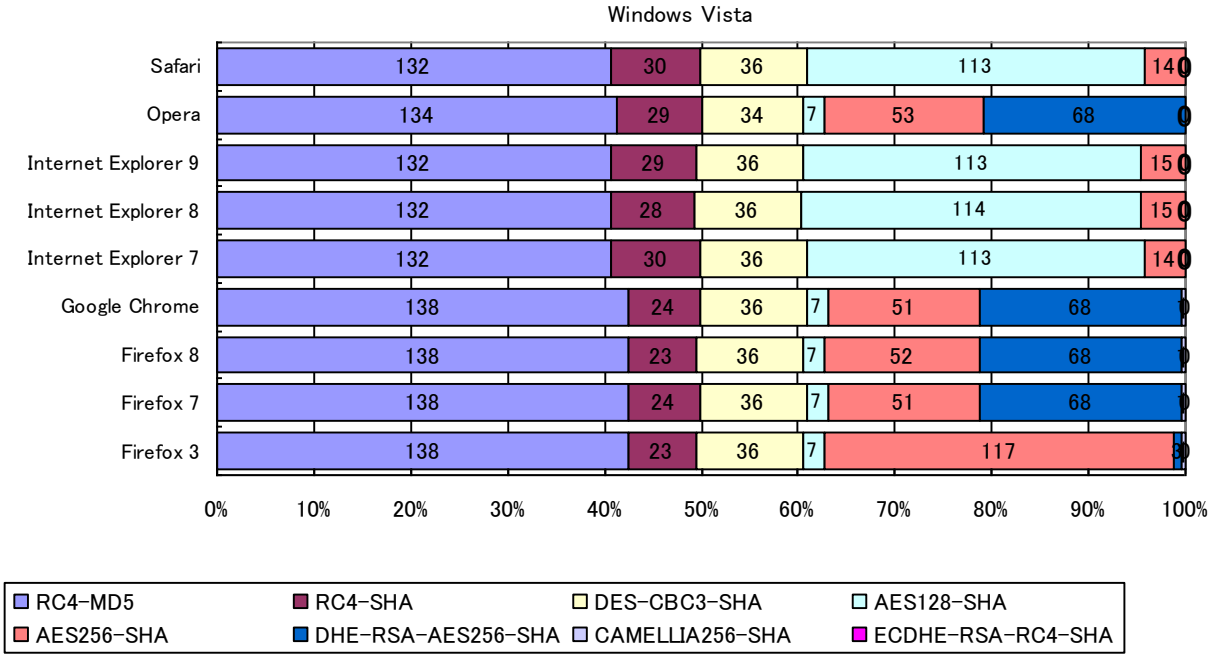
(2) Windows Vista 環境について

Windows Vista 環境において、推奨されていない Cipher suite を使った接続は、各ブラウザとも同じで、約 60%であった。

また、Windows Vista 環境において利用されている Cipher suite については、OS と各ブラウザ間で以下のような有意な相関性があった。

- Safari と Internet Explorer7 において、同一の Cipher suite が同じ率で利用されている結果であった。
- Google Chrome と Firefox7 において、同一の Cipher suite が同じ率で利用されている結果であった。

また、Internet Explorer のバージョンアップ（下表 Internet Explorer 7 から Internet Explorer 8 や Internet Explorer 9 へのバージョンアップ)、及び Firefox のバージョンアップ（下表 Firefox3 から Firefox7 や Firefox8 へのバージョンアップ）による Cipher suite の利用選択については、必ずしも推奨された暗号アルゴリズムが選択される傾向（例えば、DES から AES へ選択が移行される傾向）ではない結果となっている点に注意する必要がある。



図表：Windows Vista で接続に利用した Cipher suite <対象サーバ：325>

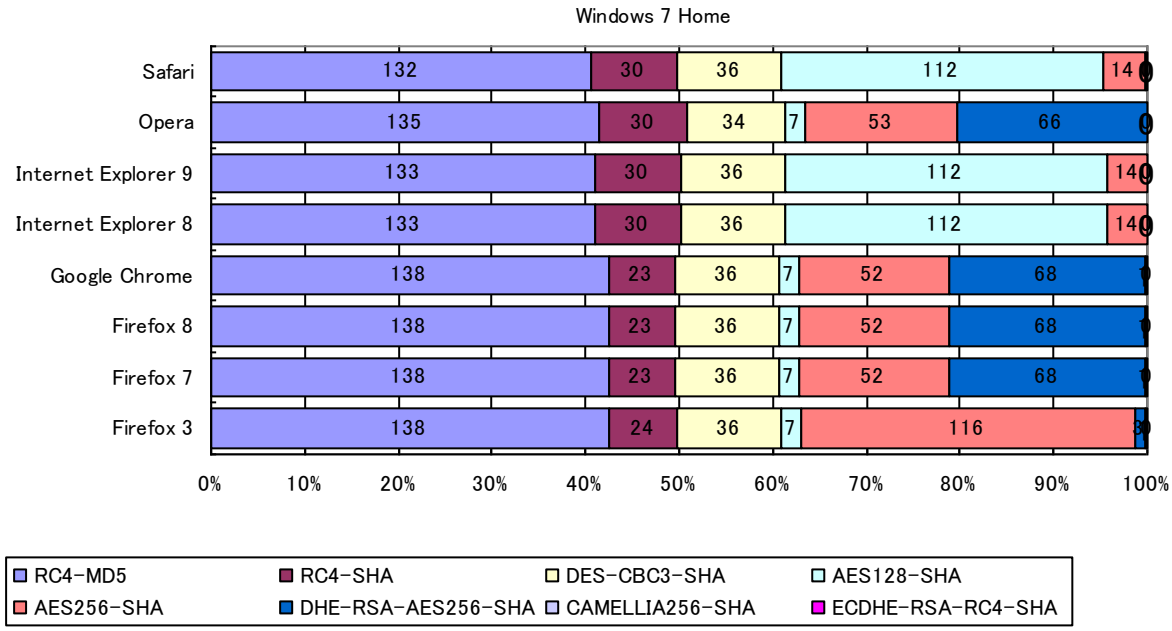
なお、Windows Vista 及び Windows 7 Home、Windows 7 Ultimate の環境では、特定の調査対象 SSL サーバについては、検証を含めた複数回の調査において、選択される Cipher suite が異なる結果となった。この理由として考えられる理由のひとつとしては、ロードバランサーの利用・設定方法が考えられる。一部の SSL サーバの設定では、サーバの負荷対策として、ロードバランサーが利用されている。ロードバランサーの利用方法としては、ロードバランサー自体で SSL のハンドシェイクから暗号化通信及び復号処理を行う場合と、Round-Robin 方式(所定のサーバに順番にリクエストを渡す方式)と Least-connectin 方式(所定のサーバのうち接続数の少ないサーバにリクエストを渡す方式)があり、これらの方式・設定などが影響し、Cipher suite の選択について設定の異なる複数のサーバが存在し、そのサーバに接続することで、結果として、Cipher suite の選択(振る舞い)が接続のタイミングによって変化したことが考えられる。
なお、一部のハウジングサービスやクラウドサービスなどでは、上記のロードバランサーのオプションも設定されているため、以前の調査に比べ、今回の調査で接続のタイミングによって、Cipher suite の選択の変化が数多く検出された可能性も考えられる。

(3) Windows 7 Home 環境について

Windows 7 Home 環境において、推奨されていない Cipher suite を使った接続は、各ブラウザとも同じで、約 60%であった。
また、Windows 7 Home 環境において利用されている Cipher suite については、OS と各ブラウザ間での以下のような有意な相関性があった。

- Safari、Internet Explorer8、Internet Explorer9 において、同一の Cipher suite が同じ率利用されている結果であった。
- Google Chrome、Firefox7、Firefox8 において、同一の Cipher suite が同じ率利用されている結果であった。

なお、前述した環境と同様に、各種のブラウザのバージョンアップによる Cipher suite の利用選択については、必ずしも推奨された暗号アルゴリズムが選択される傾向ではない結果となっている点に注意する必要がある。



図表：Windows 7 Home で接続に利用した Cipher suite <対象サーバ：325>

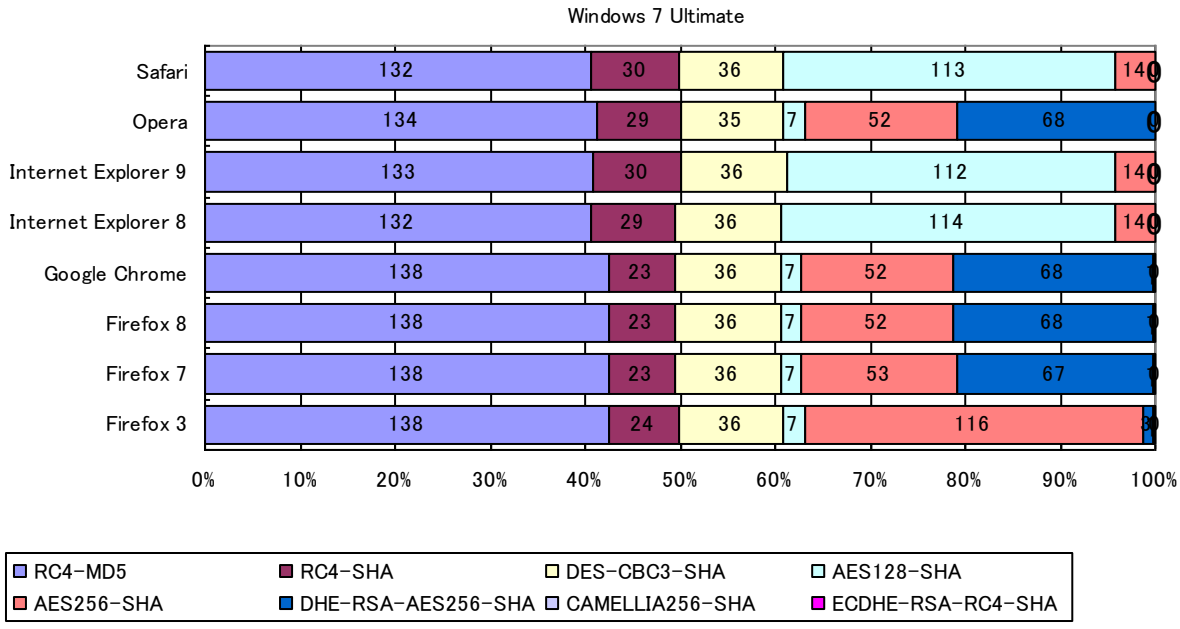
(4) **Windows 7 Ultimate 環境について**

Windows 7 Ultimate 環境において、推奨されていない Cipher suite を使った接続は、各ブラウザとも同じで、約 60%であった。

また、Windows 7 Ultimate 環境において利用されている Cipher suite については、OS と各ブラウザ間で以下のような有意な相関性があった。

- **Google Chrome、Firefox8 において、同一の Cipher suite が同じ率で利用されている結果であった。**

また、前述した環境と同様に、各種のブラウザのバージョンアップによる Cipher suite の利用選択については、必ずしも推奨された暗号アルゴリズムが選択される傾向ではない結果となっている点に注意する必要がある。

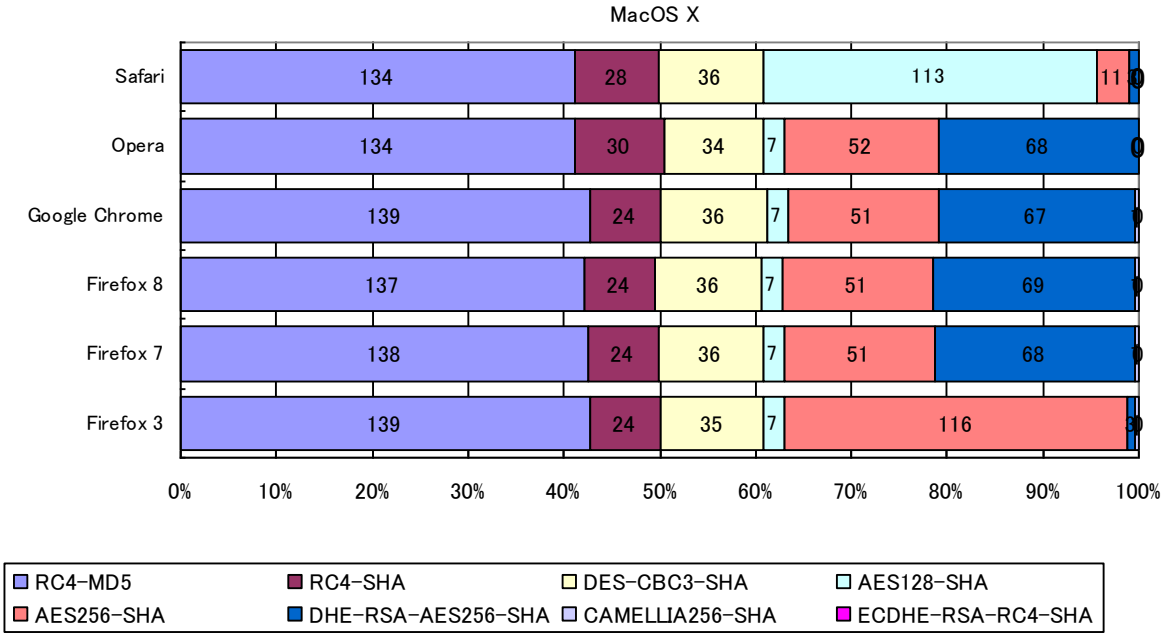


図表：Windows 7 Ultimate で接続に利用した Cipher suite <対象サーバ：325>

(5) **MAC OS X 環境について**

MAC OS X 環境において、推奨されていない Cipher suite を使った接続は、各ブラウザとも同じで、約 60%という結果であった。

また、MAC OS X 環境において利用されている Cipher suite については、OS における各ブラウザ間での有意な相関性は認められなかった。



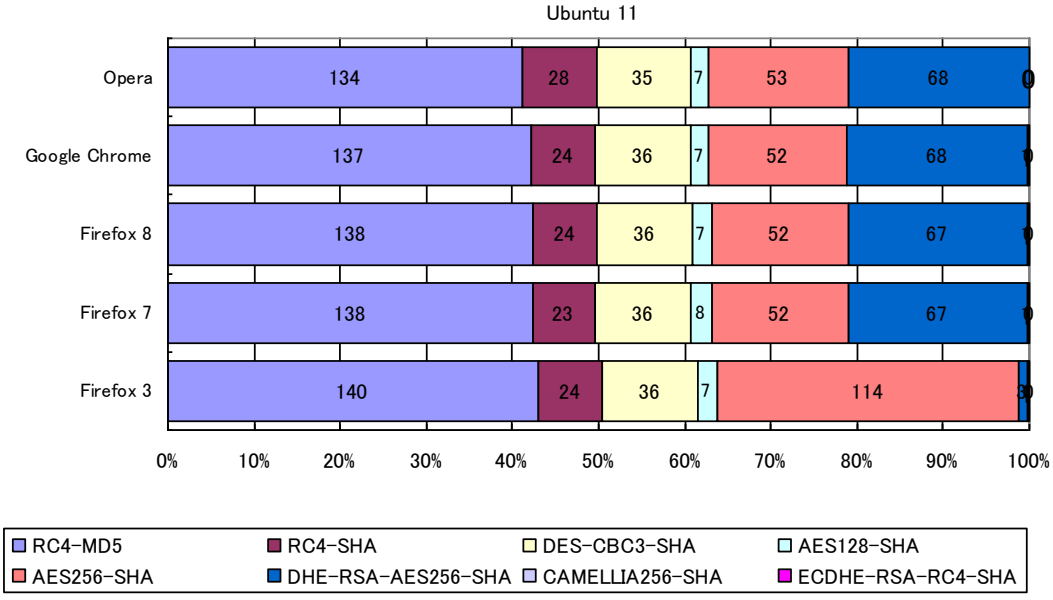
図表： MAC OS X で接続に利用した Cipher suite <対象サーバ：325>

(6) Ubuntu 環境について

Ubuntu 環境において、推奨されていない Cipher suite を使った接続は、各ブラウザとも同じで、約 60%という結果であった。

また、Ubuntu 環境において利用されている Cipher suite については、OS と各ブラウザ間での有意な相関性は認められなかった。

なお、前述した環境と同様に、各種のブラウザのバージョンアップによる Cipher suite の利用選択については、必ずしも推奨された暗号アルゴリズムが選択される傾向ではない結果となっている点に注意する必要がある。



図表： Ubuntu 11 で接続に利用した Cipher suite <対象サーバ：325>

なお、業界ごとの結果については、本書末に示す。

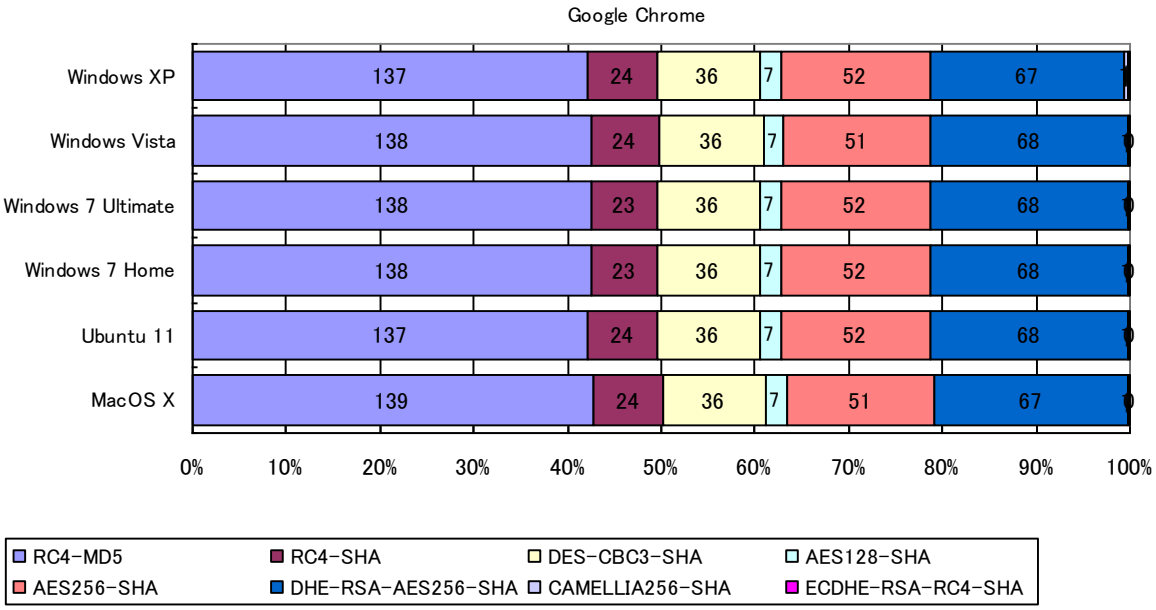
3.3.5　各ブラウザにおける調査結果

調査結果について、調査分析（３）の観点から、各ブラウザを軸として整理・分析した結果を以下に示す。

(1) Google Chrome について

Google Crome 環境において利用されている Cipher suite については、以下のような有意な相関性があった。

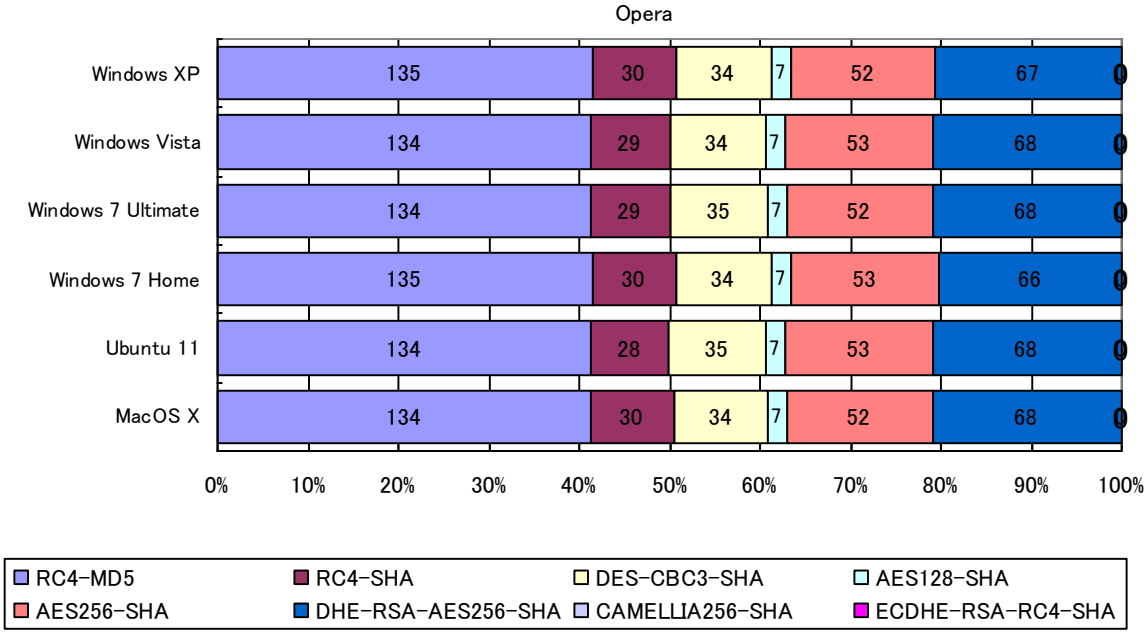
- Windows 7 Ultimate、Windows 7 Home において、同一の Cipher suite が同じ率利用されている結果であった。



図表： Google Chrome で接続に利用した Cipher suite <対象サーバ：325>

(2) Opera について

Opera 環境において利用されている Cipher suite については、ブラウザと各 OS との有意な相関性は認められなかった。

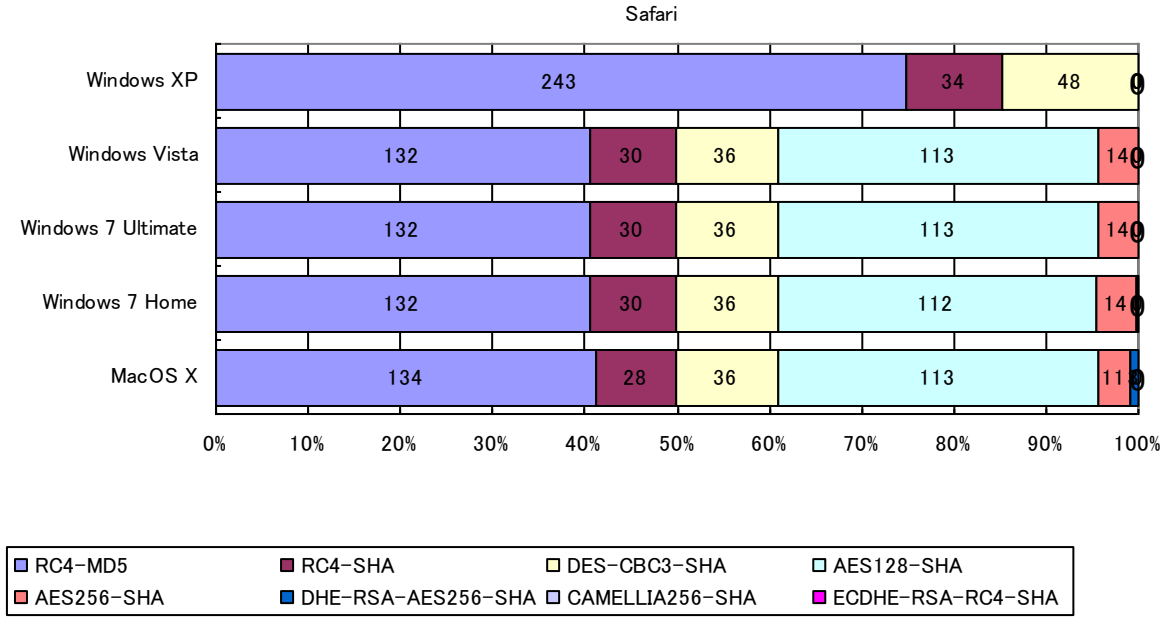


図表：Opera で接続に利用した Cipher suite <対象サーバ：325>

(3) Safari について

Safari 環境において利用されている Cipher suite については、以下のような有意な相関性があった。

- Windows Vista、Windows 7 Ultimate において、同一の Cipher suite が同じ率利用されている結果であった。

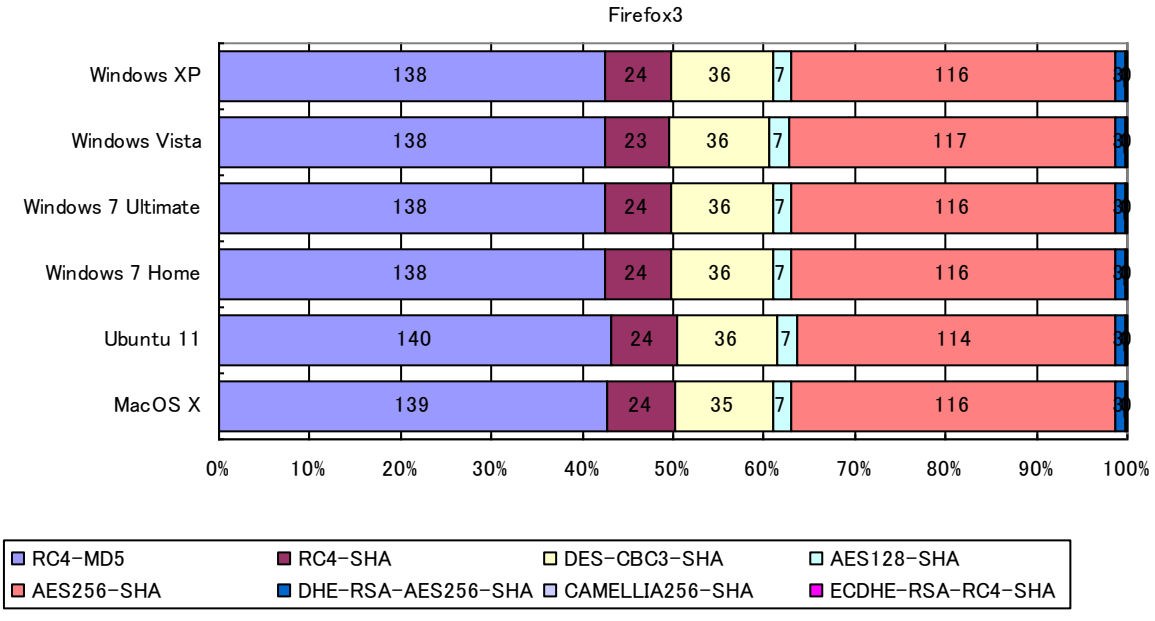


図表：Safari で接続に利用した Cipher suite <対象サーバ：325>

(4) Firefox 3 について

Firefox 3 環境において利用されている Cipher suite については、以下のような有意な相関性があった。

- Windows Vista、Windows 7 Ultimate、Windows 7 Home において、同一の Cipher suite が同じ率利用されている結果であった。

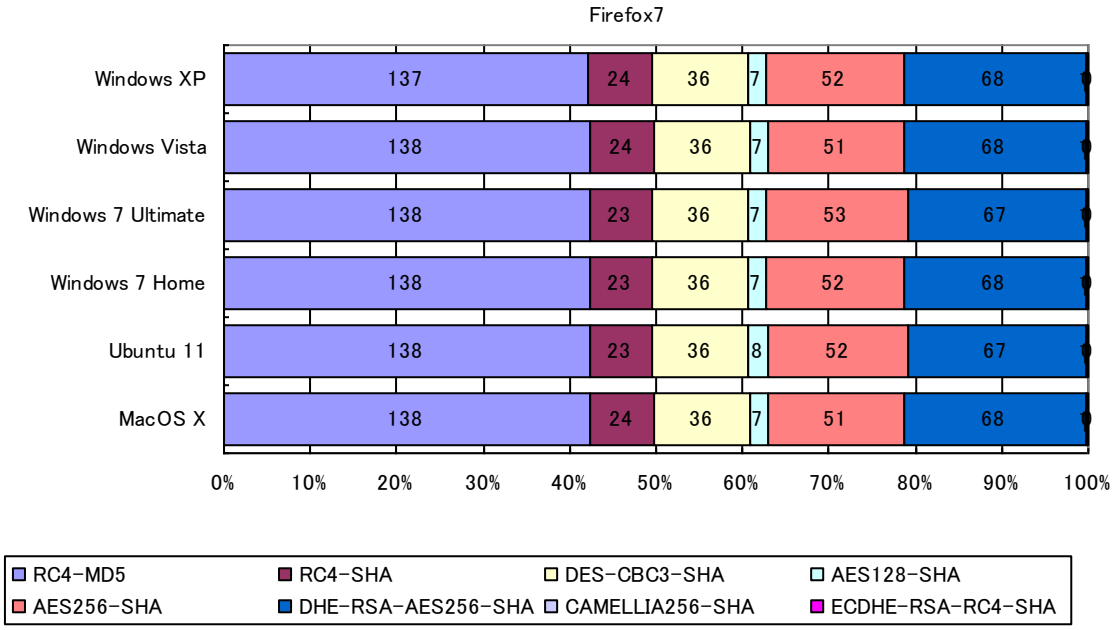


図表： Firefox 3 で接続に利用した Cipher suite <対象サーバ：325>

(5) Firefox 7 について

Firefox 7 環境において利用されている Cipher suite については、以下のような有意な相関性があった。

- Windows Vista、Mac OS X において、同一の Cipher suite が同じ率利用されている結果であった。

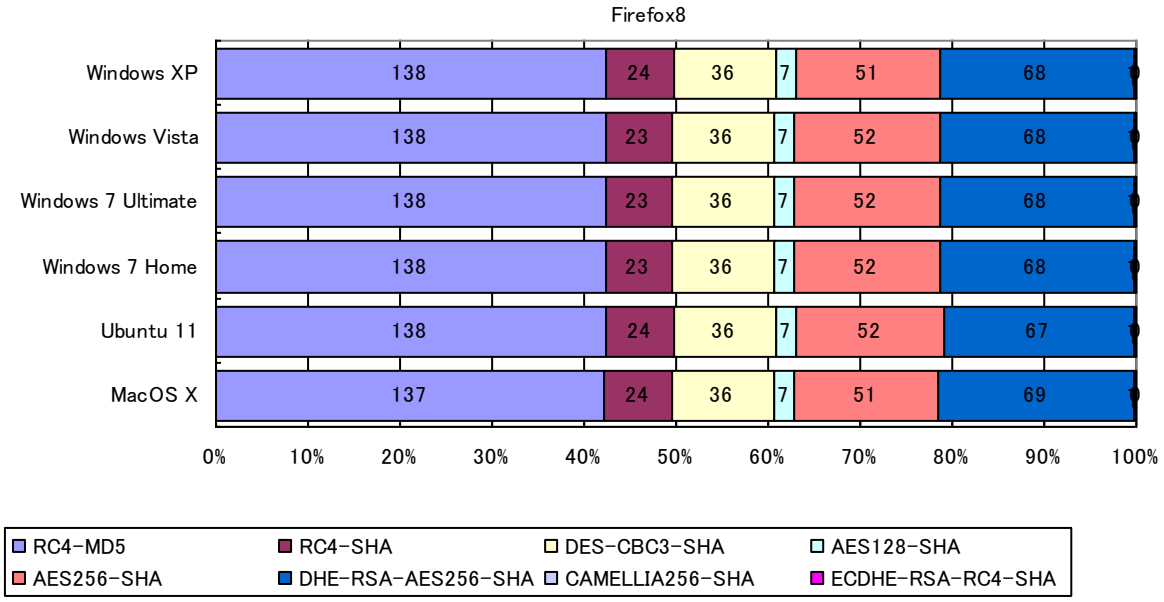


図表： Firefox 7 で接続に利用した Cipher suite <対象サーバ：325>

(6) Firefox 8 について

Firefox 8 環境において利用されている Cipher suite については、以下のような有意な相関性があった。

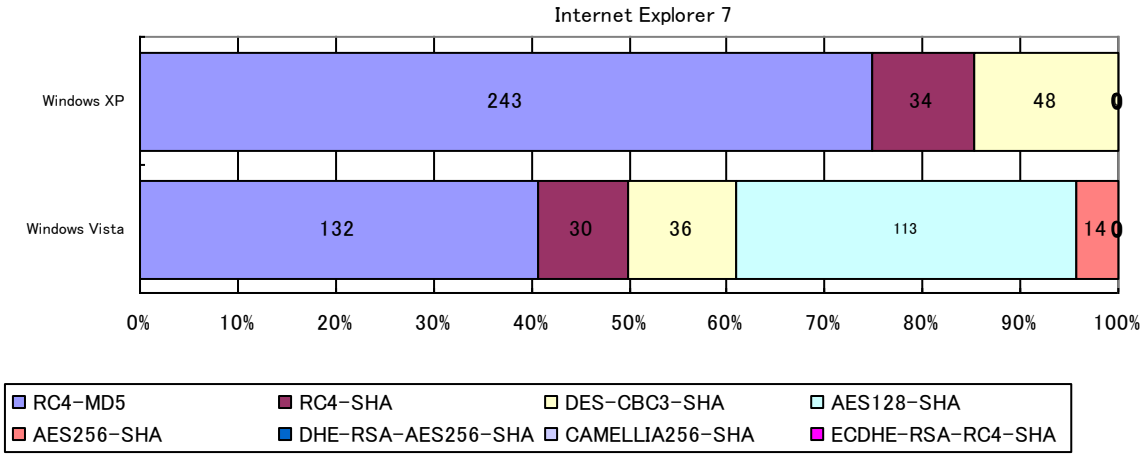
- Windows Vista、Windows 7 Ultimate、Windows 7 Home において、同一の Cipher suite が同じ率利用されている結果であった。



図表： Firefox 8 で接続に利用した Cipher suite <対象サーバ：325>

(7) Internet Explorer 7 について

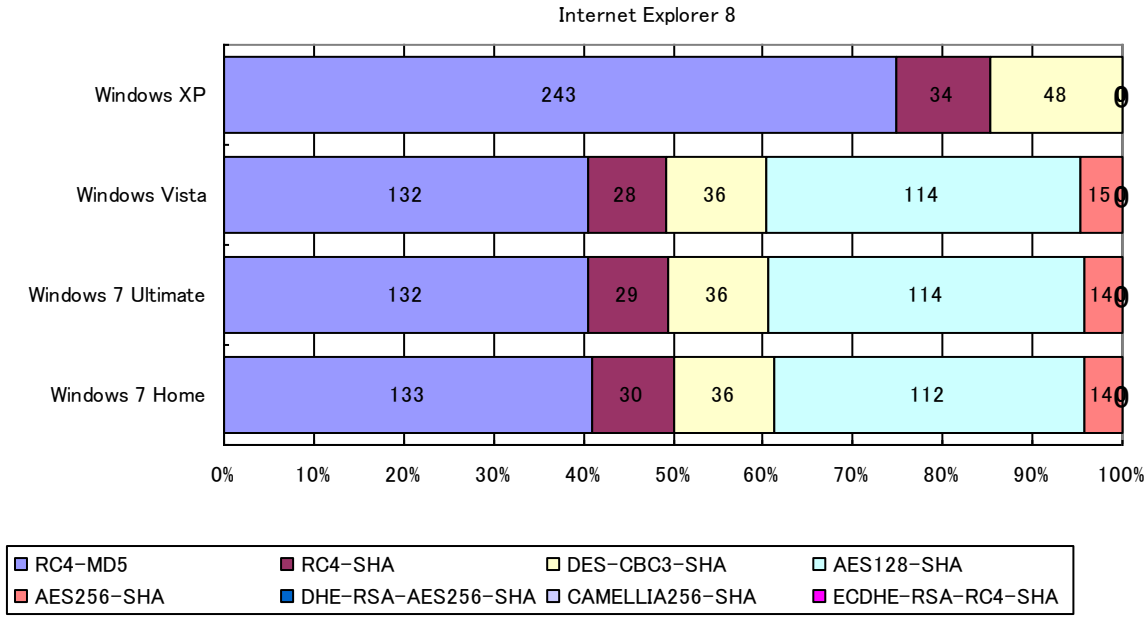
Internet Explorer 7 環境において利用されている Cipher suite については、ブラウザと各 OS との有意な相関性は認められなかった。



図表：Internet Explorer 7 で接続に利用した Cipher suite <対象サーバ：325>

(8) Internet Explorer 8 について

Internet Explorer 8 環境において利用されている Cipher suite については、ブラウザと各 OS との有意な相関性は認められなかった。

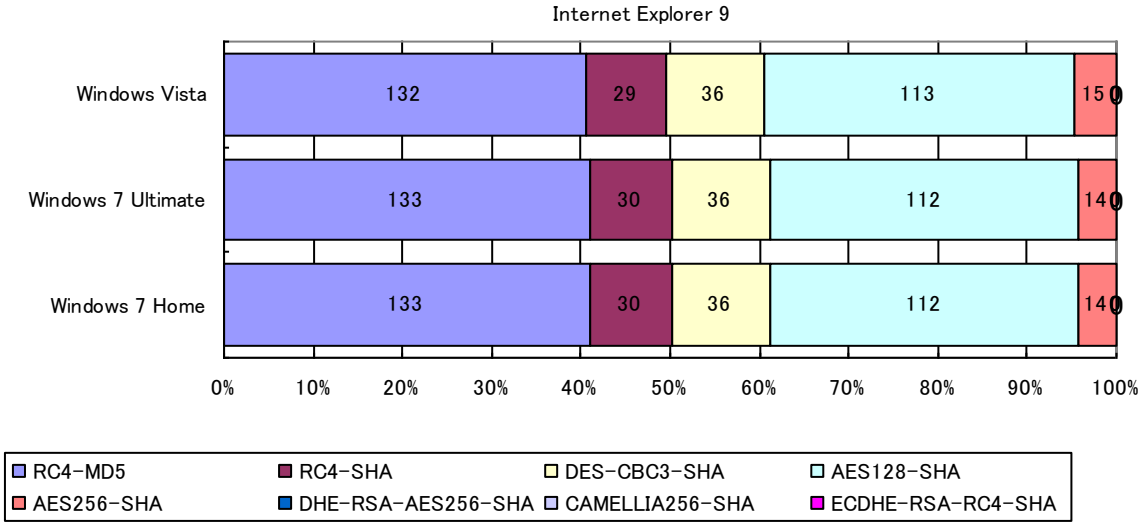


図表：Internet Explorer 8 で接続に利用した Cipher suite <対象サーバ：325>

(9) Internet Explorer 9 について

Internet Explorer 9 環境において利用されている Cipher suite については、以下のような有意な相関性があった。

- Windows 7 Ultimate と Windows 7 Home において、同一の Cipher suite が同じ率利用されている結果であった。

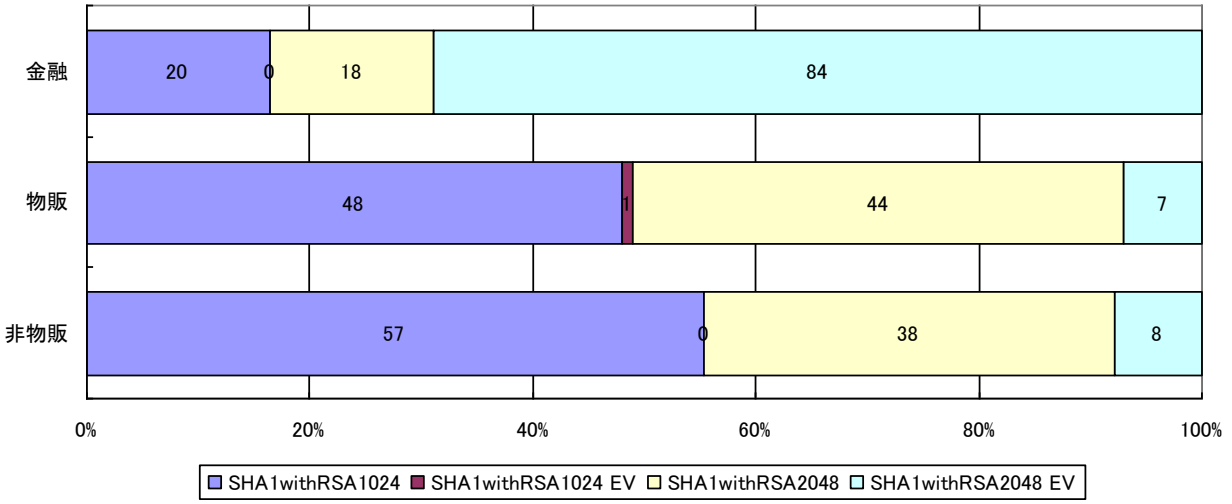


図表：Internet Explorer 9 で接続に利用した Cipher suite <対象サーバ：325>

なお、業界ごとの結果については、本書末に示す。

3.4　ＳＳＬサーバ証明書調査結果

ＳＳＬサーバ証明書を調査した結果、ＳＳＬサーバ証明書の期限切れ等の重大な瑕疵は無かった。また、EV-SSL 証明書の利用については、以下のような結果であった。金融系は、69%と 3 業界の中で最も高く、物販系及び非物販系はともに 8%であった。



図表： EV-SSL 証明書の利用結果（3 業界）<対象サーバ：325>

(1) 金融系について

金融系では、EV-SSL 証明書の利用が 69%、EV-SSL でない証明書の利用が 31%であり、EV-SSL 証明書の利用率は、3 業界中で最も高い利用率であった。EV-SSL 証明書の利用率が高いことから、サービス主体の身元証明などが他業界に求められていることがわかる。また、すべての EV-SSL 証明書は、RSA2048 であり、RSA1024 の EV-SSL 証明書ではない。なお、詳細結果については別紙調査シートを参照。

(2) 物販系について

物販系では、EV-SSL 証明書の利用が 8%、EV-SSL でない証明書の利用が 92%であり、EV-SSL 証明書の利用率は、非物販系と同数であった。また、EV-SSL 証明書は RSA2048 が 7%と高いが、RSA1024 も存在する。EV-SSL ではない証明書については、RSA2048 と RSA1024 がほぼ同数である。なお、詳細結果については別紙調査シートを参照。

(3) 非物販系について

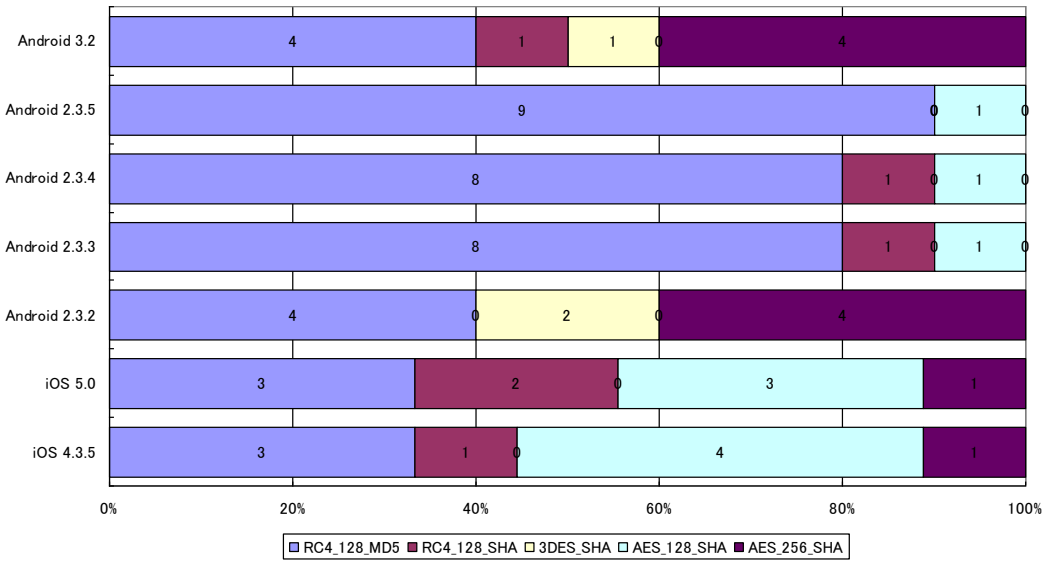
非物販系では、EV-SSL 証明書の利用が 8%、EV-SSL でない証明書の利用が 92%であり、EV-SSL 証明書の利用率は、物販系と同数である。SV-SSL 証明書は、金融系と同じく、すべて RSA2048 であり、RSA1024 は存在しない。また、他の業界と比較では、EV-SSL ではない証明書の RSA1024 が 55%であり、3 業界の中で最も高い。なお、詳細結果については別紙調査シートを参照。

3.5　携帯デバイスを用いた調査結果

携帯デバイスを用いた調査の結果、携帯キャリアによる有意な差は存在しなかったため、各携帯デバイスの OS における調査結果を下表に示す。この結果から、推奨されている暗号アルゴリズムのみで構成された Cipher suite が利用されている率は低く、各 OS がバージョンアップされたにも関わらず、推奨されていない暗号アルゴリズムを用いた Cipher suite が利用されている傾向にある。

また、比較的新しい各携帯デバイス OS で推奨されている暗号アルゴリズムのみで構成されている Cipher suite を利用している企業やサイトでは、旧バージョンであっても推奨されている暗号アルゴリズムのみで構成されている Cipher suite を利用しているため、企業やサイトによる差が顕著である。

具体的な Cipher suite の利用状況については、iOS4.3.5 を除いて、各デバイスの推奨されていない Cipher suite の利用率は、50%以上であり、Android2.3.3、Android2.3.4、Android2.3.5 では、90%であった。



図表：携帯デバイスを用いた調査結果概要 <対象サーバ：10>

4. まとめ

本調査では、SSL サーバの設定状況を調査するために、SSL サーバのデフォルト設定と実際の SSL サーバの設定状況の調査を行った。SSL サーバのデフォルト設定の調査では、15 種類の想定サーバ構成と 38 種類の想定クライアント環境について、サポートする Cipher suite の一覧とデフォルト設定時の Cipher suite の優先順位について調査した。また、実際の SSL サーバの設定状況の調査では、金融系、物販系、非物販系の 3 業界について、合計 300 以上の SSL サーバに対して、想定サーバ構成を考慮した Cipher suite 個別の通信可否確認、及び想定クライアント環境において接続する際の Cipher suite を確認した。

調査の結果、推奨された共通鍵暗号アルゴリズム及びメッセージ認証のみで構成された Cipher suite を利用可能な比率は低く、これらの利用可能な比率や EV-SSL 証明書の利用状況などは、業界ごとに異なる結果であった。オンラインショッピングなど SSL プロトコルを利活用する関係者は数多く存在し、その立場も異なるため、安全な利用における合意形成が難しいが、少なくとも以下の検討が必要である。

- 利用者について
  - SSL プロトコルを安全に利用するために、ブラウザの設定や OS の設定等の情報が必要である。また、ブラウザの設定で、OS の設定を参照する場合は、その内容を明記するとともに、設定参照先の確認方法についても明記する必要がある。
  - SSL プロトコルを安全に利用するために、SSL サーバ証明書を確認することを普及啓発する必要がある。

- SSL サーバ設計・構築
  - 想定する接続対象デバイスや OS/ブラウザ等で安全に SSL プロトコルを利用できることを確認し、その確認内容に基づいて設定・構築する必要がある。
  - 上記で安全に SSL プロトコルを利用できない接続対象デバイスや OS/ブラウザ等においても SSL プロトコルを利用する必要もあると考えられる。例えば、古い携帯デバイスや、古いブラウザなどで SSL プロトコルを利用する場合が想定されるが、このような場合には、接続先のクライアントに対して、安全に SSL プロトコルを利用できない環境であること、または安全に SSL プロトコルを利用できるクライアント環境への移行を推奨することを示す必要がある。

- SSL サーバ運用・管理
  - 証明書については、運営主体者が正しく設定されていること。また、運営主体者と異なる場合は、その旨を表示（告知）する必要がある。
  - Web ページの構成（フレーム等を用いて）などで http と https の同一ページに構成されていないことを確認し、http と https が同一ページに構成されないように確認、管理する必要がある。
  - 利用者の重要情報には、ID やパスワードも含めることを意識し、ID やパスワードも含む利用者の重要情報を守るために、ログイン画面後に SSL プロコトルを利用するのではなく、利用者の重要情報を送信するログイン画面が SSL プロコトルを利用できるように、https で提供されていることを確認し、必要に応じて修正する必要がある。

以上の SSL プロトコルを利活用する関係者の合意形成および検討事項以外にも、本調査で得られた SSL サーバ設定状況が、今後の安全な普及発展のために利用されることになれば幸いである。

5. 参照文献

[1] 神田雅透、「TLS/SSL の暗号利用に関する現状と課題」、Internet week 2009
http://www.nic.ad.jp/ja/materials/iw/2009/proceedings/h9/iw2009-h9-04.pdf

[2] 神田雅透、山岸篤弘、「暗号世代交代についての暗号学会とビジネスサイドのギャップをどう埋めるか ～ SSL サーバの暗号設定の現状からの考察 ～」、2009 年暗号と情報セキュリティシンポジウム SCIS 2009, 2009

[3] 第 17 回情報セキュリティ政策会議（内閣官房情報セキュリティセンター）,"政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針,"2008
http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf

[4] CRYPTREC, "電子政府推奨暗号の利用方法に関するガイドブック," 2008
http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

[5] NIST SP800-44 Version 2, "Guidelines on Securing Public Web Servers," 2007
http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

[6] 松本泰、宇根正志、「SSL 証明書における暗号アルゴリズム移行の現状と今後の対応」、2010-J-11
http://www.imes.boj.or.jp/research/papers/japanese/10-J-11.pdf

[7] 田村裕子、「ISO/TC68 における金融分野向け推奨暗号アルゴリズムの検討状況」、2008-J-21
http://www.imes.boj.or.jp/research/papers/japanese/08-J-21.pdf

[8] 宇根正志、神田雅透、「暗号アルゴリズムにおける 2010 年問題について」、2005-J-22
http://www.imes.boj.or.jp/research/papers/japanese/05-J-22.pdf

[9] 神田雅透、「政府期間及び金融機関の SSL サーバ暗号設定に関する調査結果について」、PKI Day2009
http://www.jnsa.org/seminar/2009/0624/data/07_kanda.pdf

[10] 神田雅透、「暗号アルゴリズムの安全性のお話」、Internet Week 2008
http://www.nic.ad.jp/ja/materials/iw/2008/proceedings/H10/IW2008-H10-01.pdf

[11] NIST SP800-131A "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths," 2011
http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

6. 用語・略語集

a. **電子政府推奨暗号（リスト）**
各府省が情報システムの構築にあたって暗号アルゴリズムを利用する場合には、可能な限り、利用を促進する目的で選定された暗号アルゴリズム（また、その一覧表）。

b. CRYPTREC (Cryptography Research and Evaluation Committees)
電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討する、総務省及び経済産業省のプロジェクト

c. NIST (National Institute of Standards and Technology)
米国立標準技術研究所。米国商務省の傘下にあり、情報セキュリティに関する幅広い米国政府標準やガイドラインの作成等を行っている

d. IETF (Internet Engineering Task Force)
インターネットにおける標準規格を策定する団体

e. SSL (Secure Socket Layer)
インターネット上で通信を安全に行うためのプロトコルの一種。ネットスケープコミュニケーションズ社が開発したプロトコルであり、その後、IETF において標準化された。現在のブラウザにはデフォルトで搭載されている

f. TLS (Transport Layer Security)
SSL **と同様で、インターネット上で通信を安全に行うためのプロトコルの一種。**TLS 1.0 **はネットスケープコミュニケーションズ社が開発した** SSL 3.0 **を改良したプロトコルであり、**IETF **で** RFC 2246 **として標準化されている**

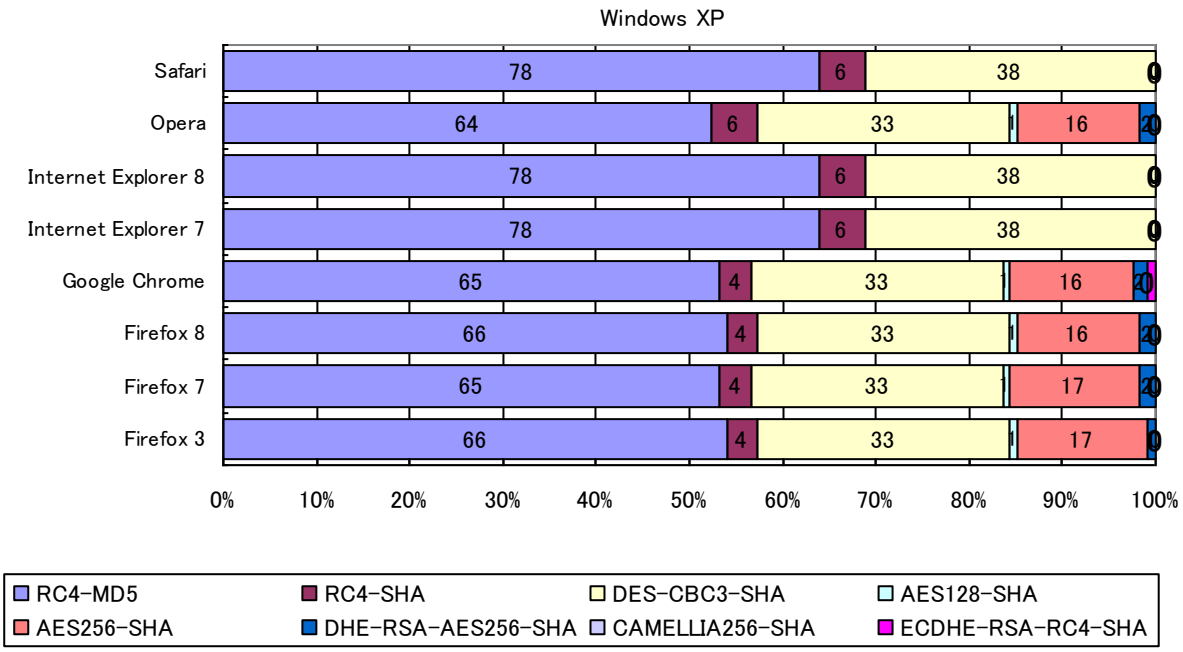
g. EV-SSL (Extended Validation Secure Sockets Layer)
SSL **の問題点を改善するために、強化された** SSL

h. EV-SSL **証明書**
認証局や Web **ブラウザ・ベンダー等で構成された業界団体「**CA/Browser **フォーラム」において発行された「**EV（extended validation）**証明書ガイドライン」によって、企業の実在性の確認、ドメイン名情報の確認など身元情報をより厳格に審査をしたうえで発行する証明書**

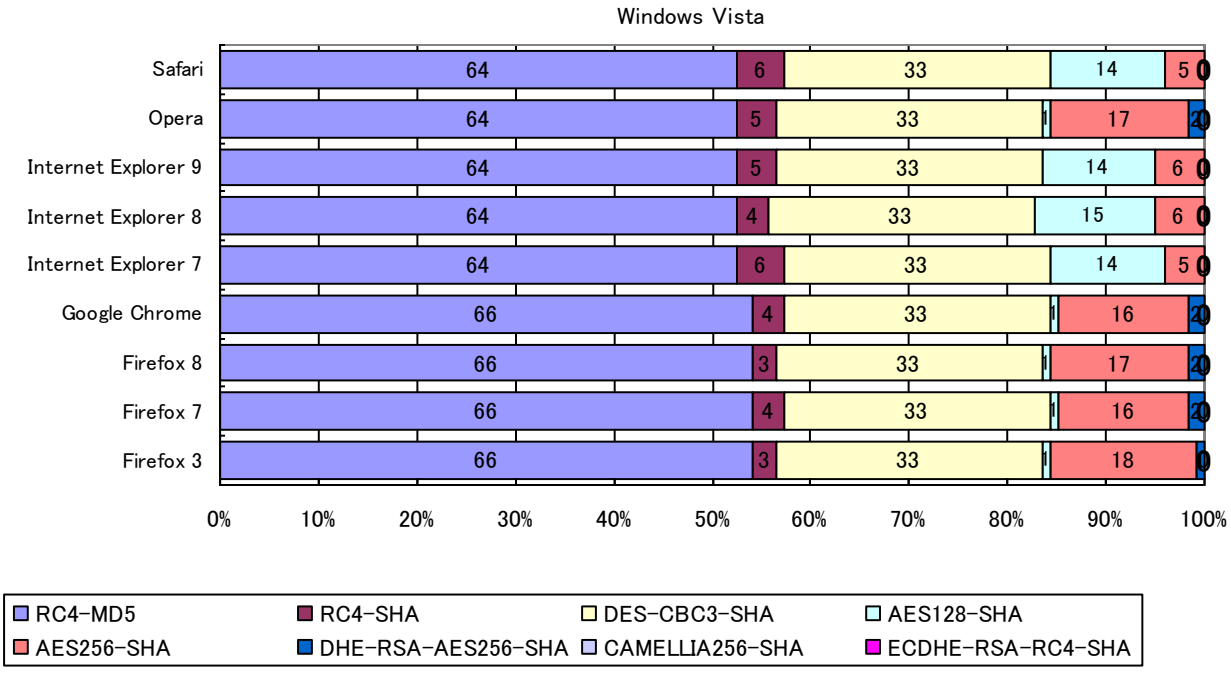
i. Cipher suite
SSL **プロトコルで利用する暗号アルゴリズムの組み合わせ。共通鍵暗号、公開鍵暗号、ハッシュ関数等の組み合わせで構成され、**IETF **によって組み合わせごとに番号が一意に決められている。ブラウザと** SSL **サーバが当該番号をやり取りすることによって、利用する暗号アルゴリズムを決定する**

j. SSL **サーバ証明書**
SSL **サーバのなりすまし防止とブラウザとの鍵交換のために用いられる、信頼できる第三者機関（認証局）が発行した証明書**

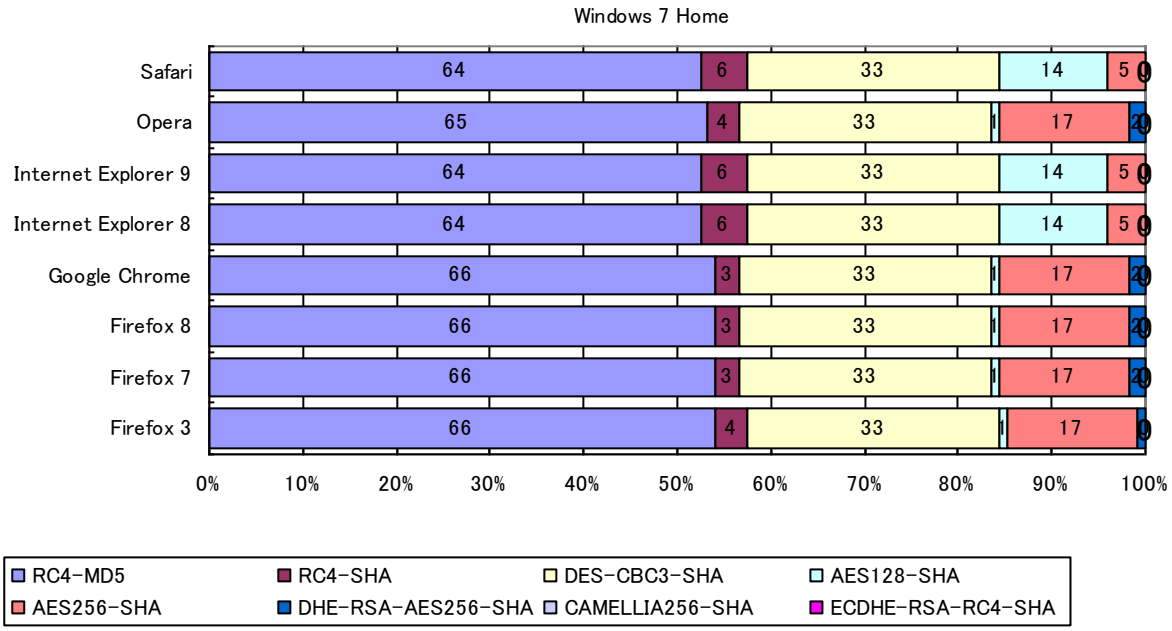
金融系詳細



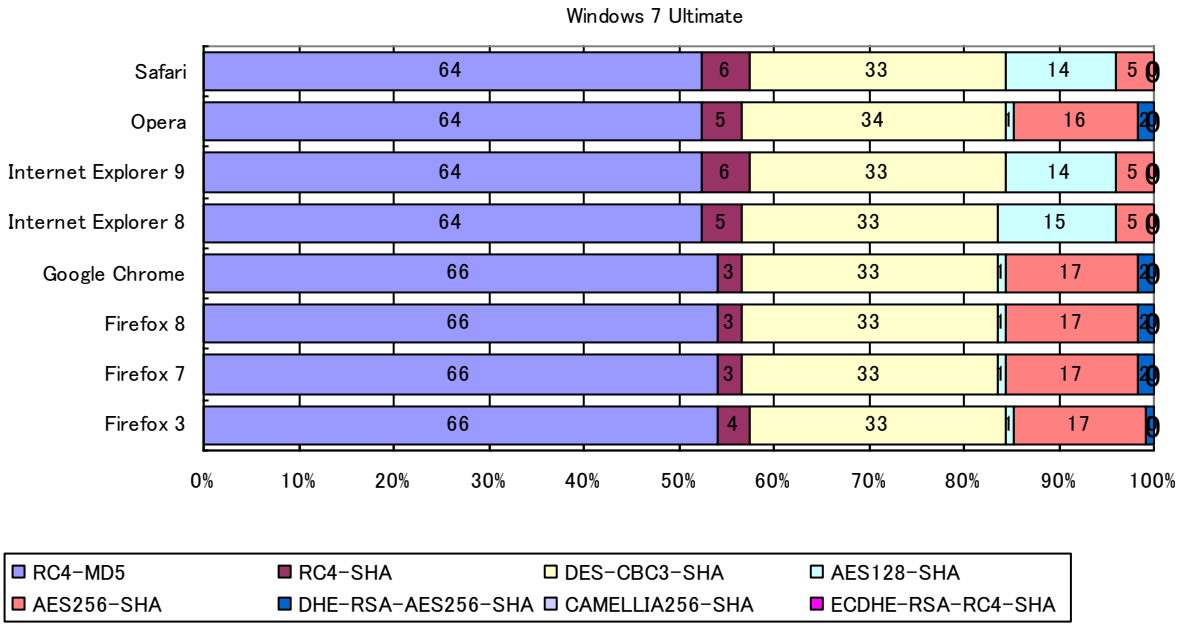
図表：Windows XP **で接続に利用した** Cipher suite <**金融系：**122 **サーバ**>



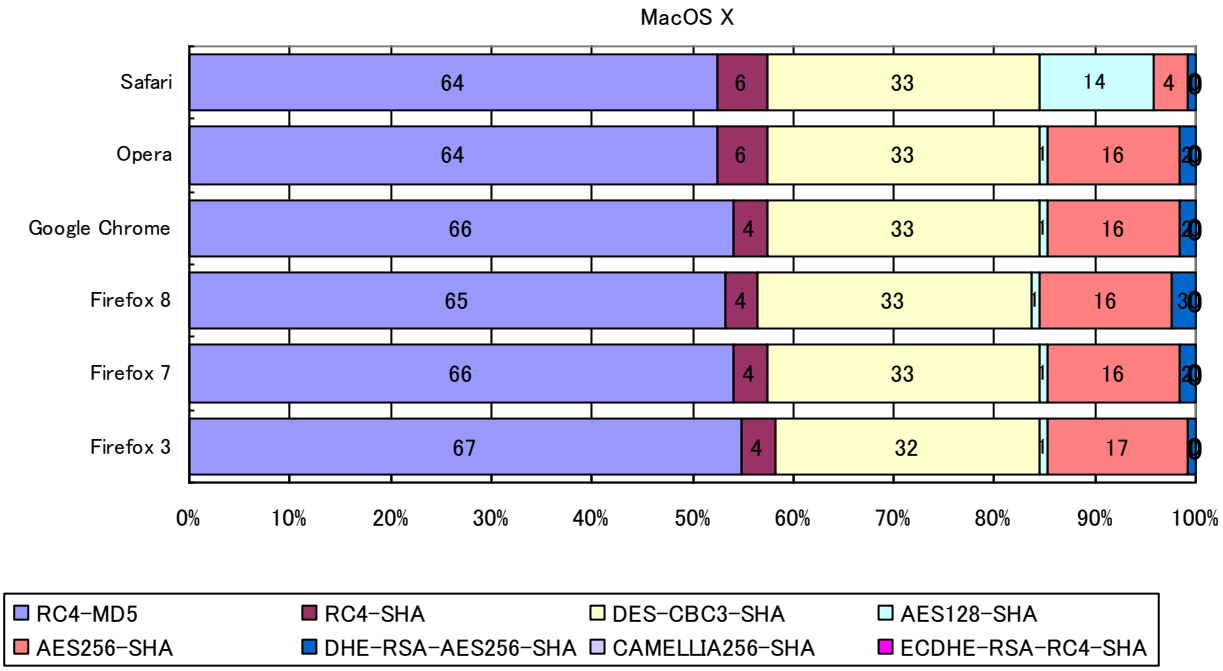
図表：Windows Vista **で接続に利用した** Cipher suite <**金融系：**122 **サーバ**>



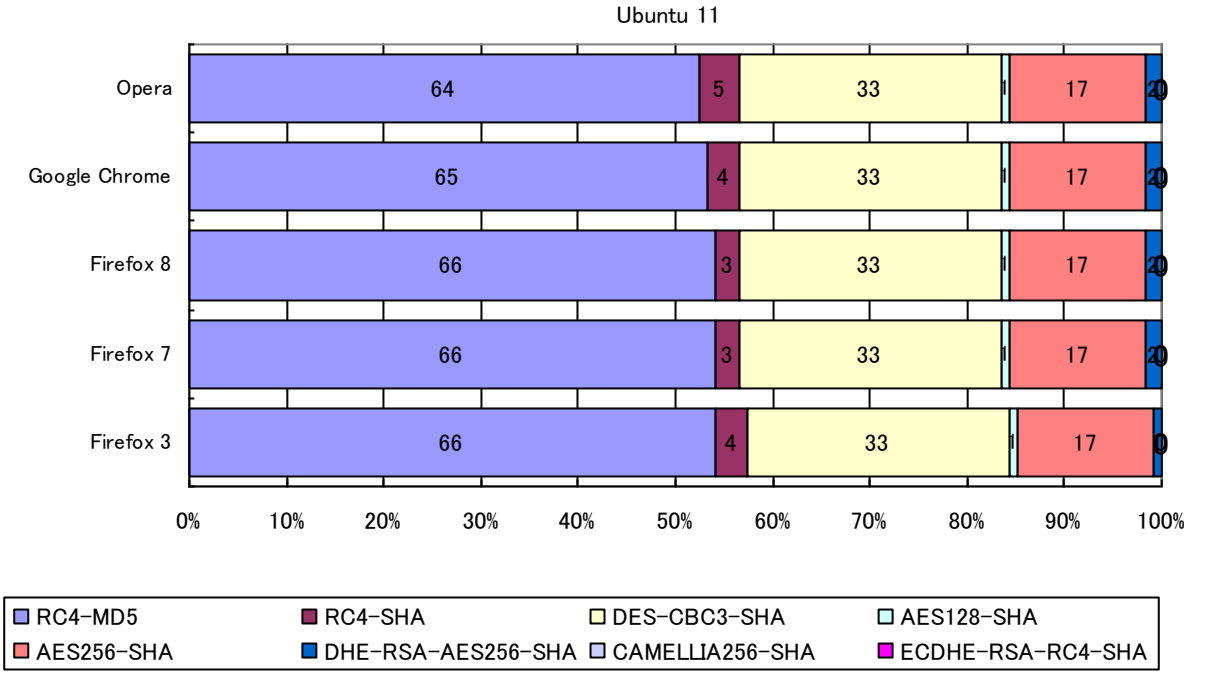
図表：Windows 7 Home で接続に利用した Cipher suite <金融系：122 サーバ>



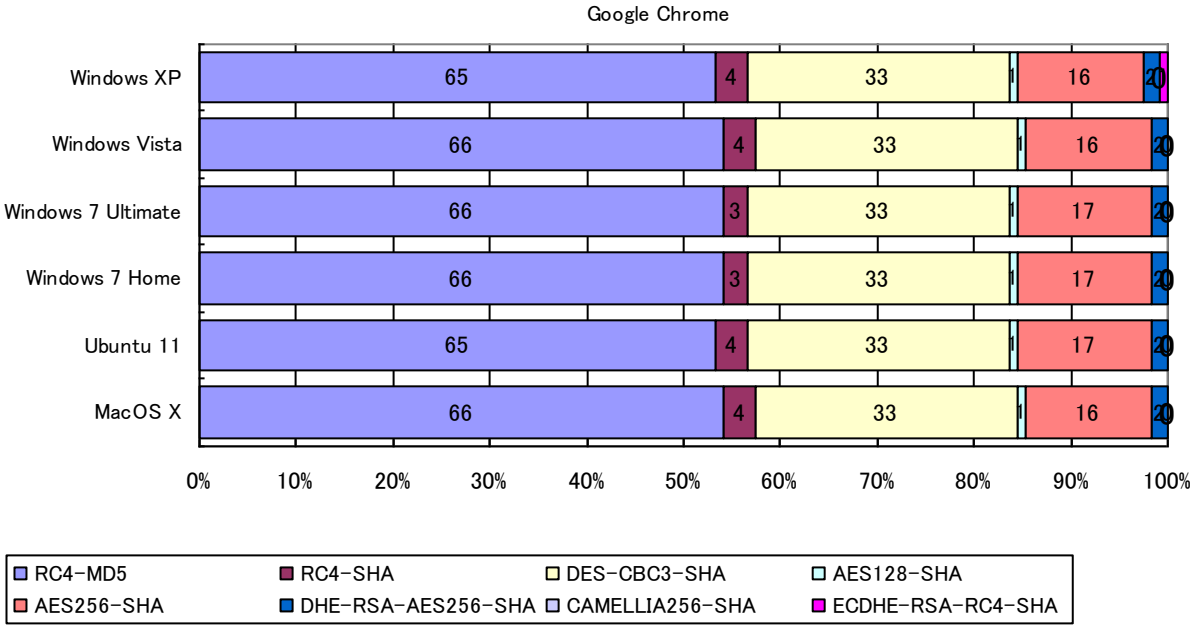
図表：Windows 7 Ultimate で接続に利用した Cipher suite <金融系：122 サーバ>



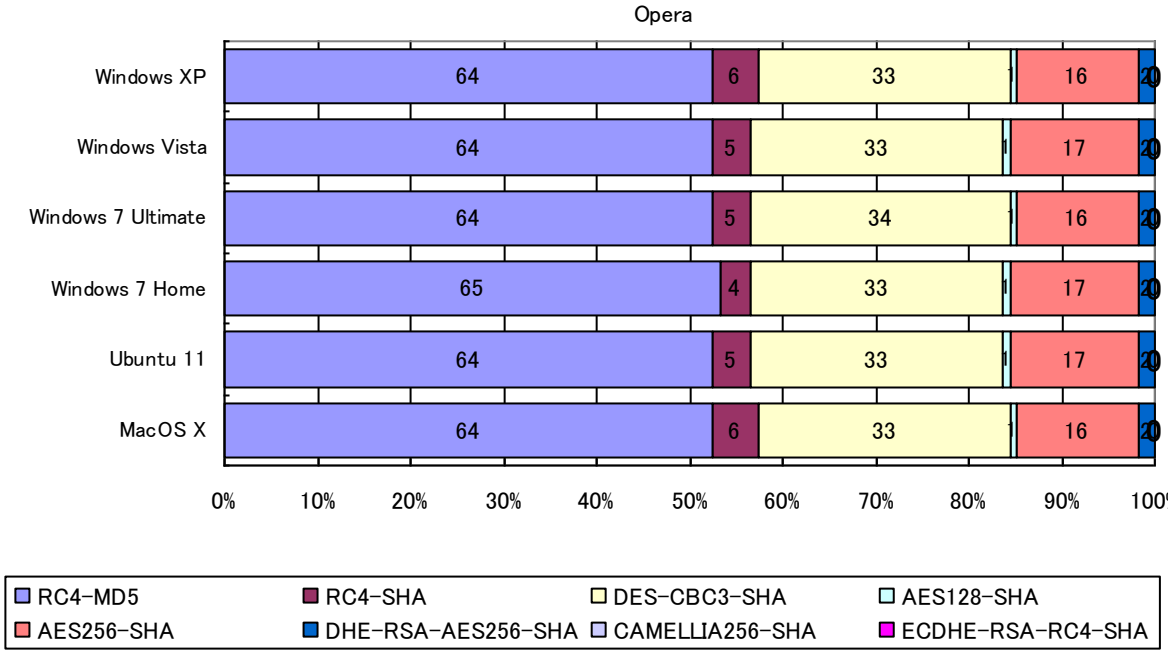
図表： MAC OS X **で接続に利用した** Cipher suite <**金融系：**122 **サーバ**>



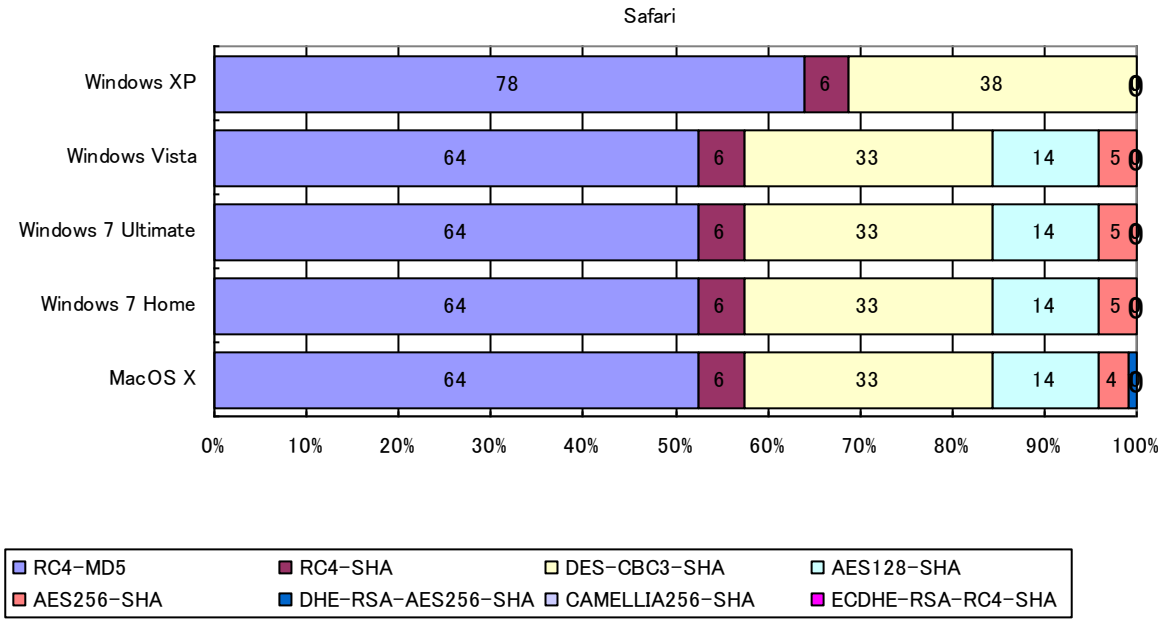
図表： Ubuntu 11 **で接続に利用した** Cipher suite <**金融系：**122 **サーバ**>



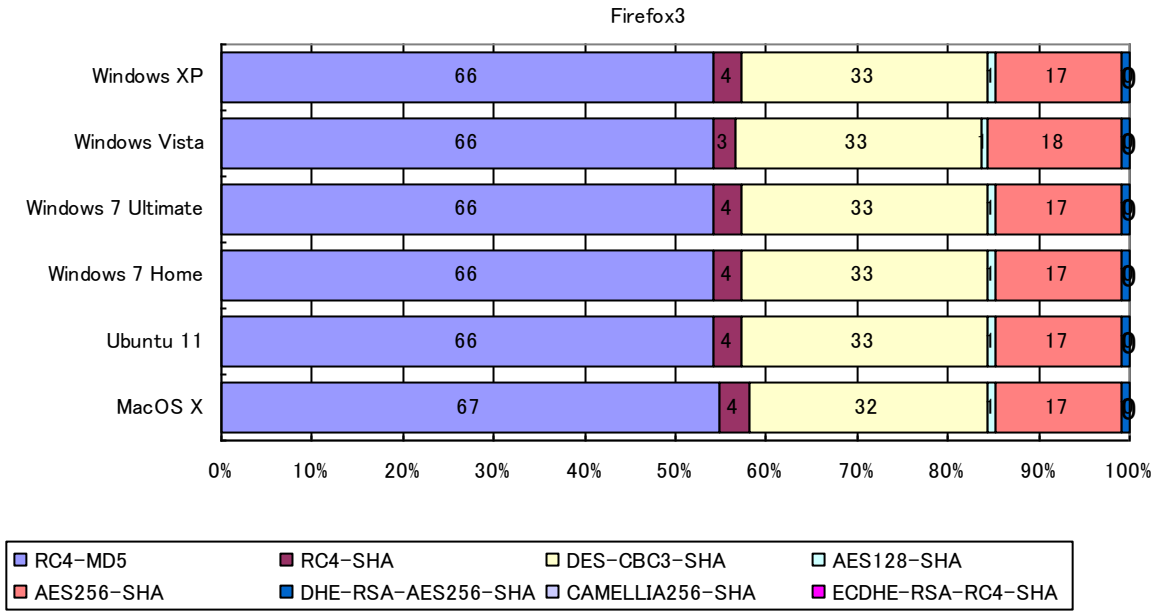
図表： Google Chrome **で接続に利用した** Cipher suite <**金融系：**122 **サーバ**>



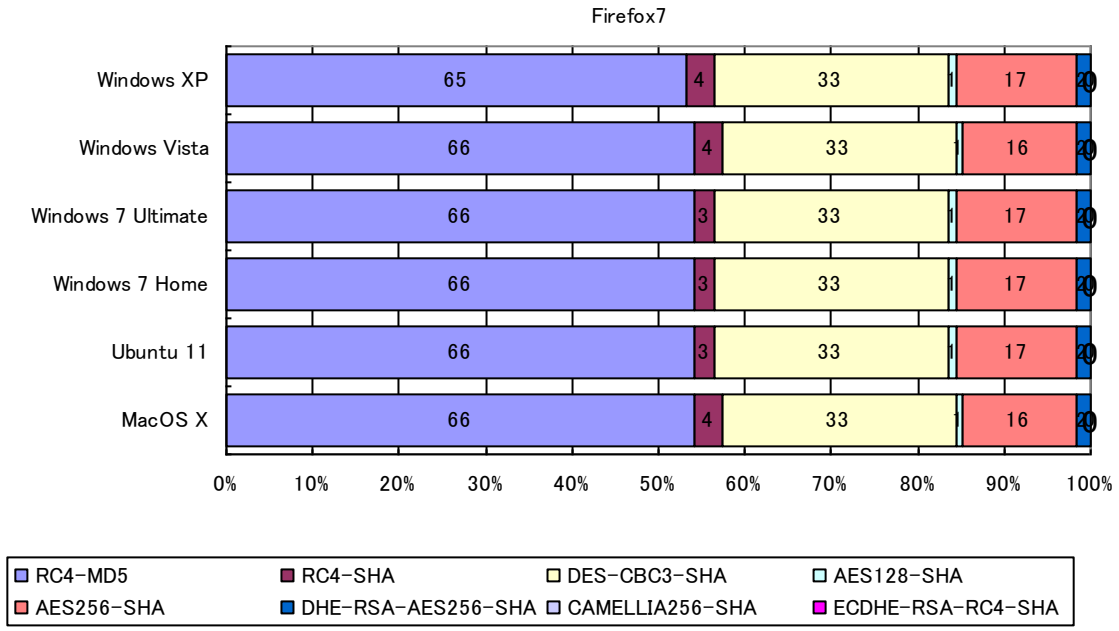
図表：Opera **で接続に利用した** Cipher suite <**金融系：**122 **サーバ**>



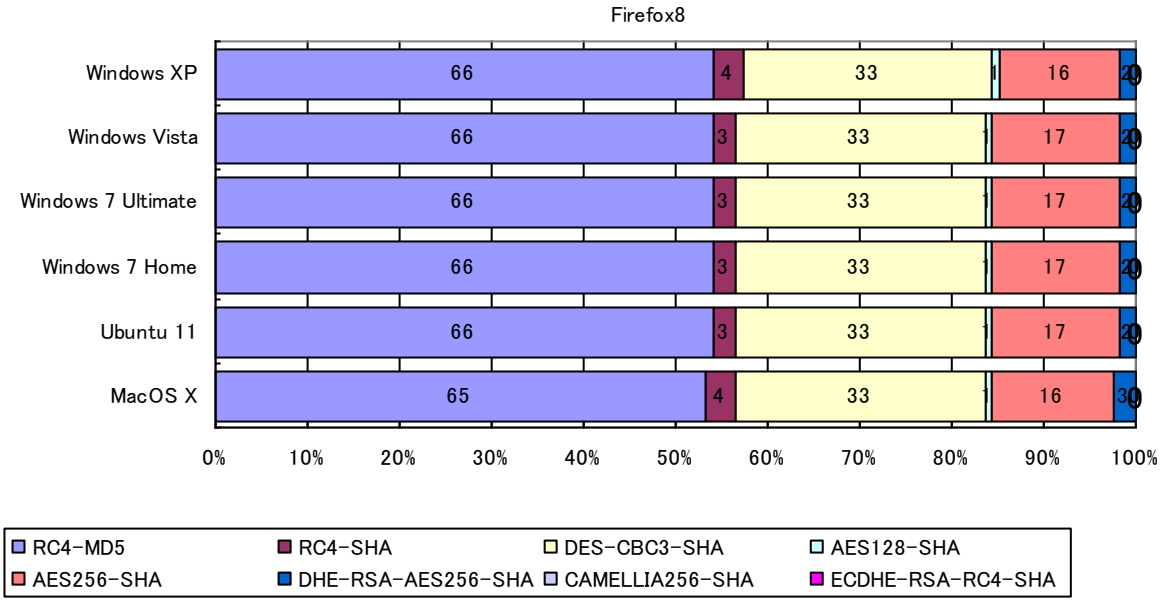
図表：Safari で接続に利用した Cipher suite <金融系：122 サーバ>



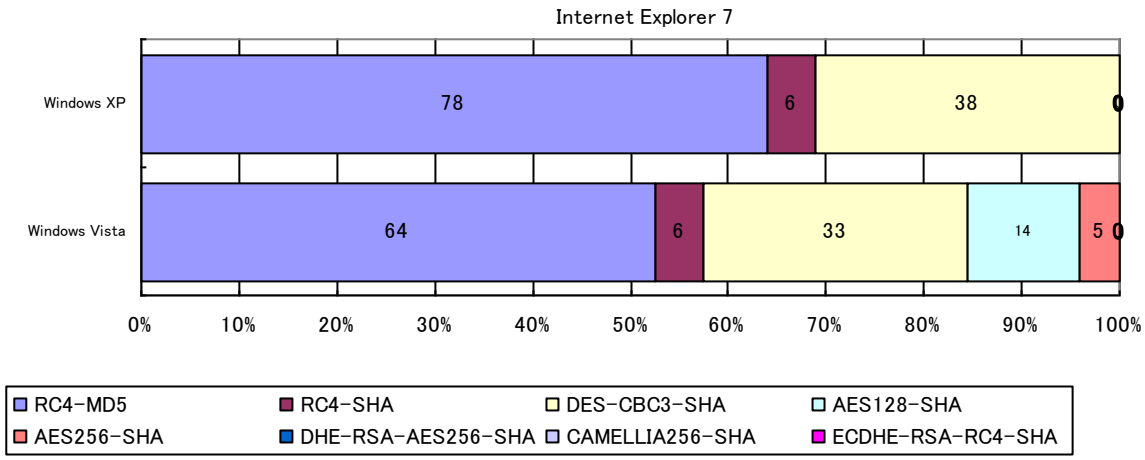
図表： Firefox 3 で接続に利用した Cipher suite <金融系：122 サーバ>



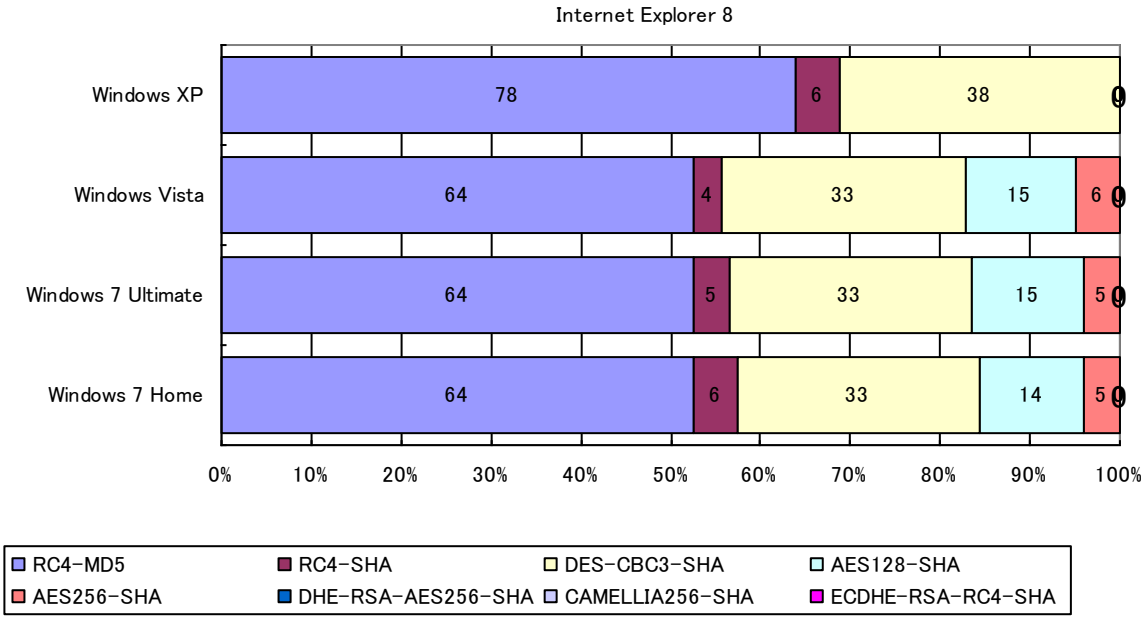
図表： Firefox 7 で接続に利用した Cipher suite <金融系：122 サーバ>



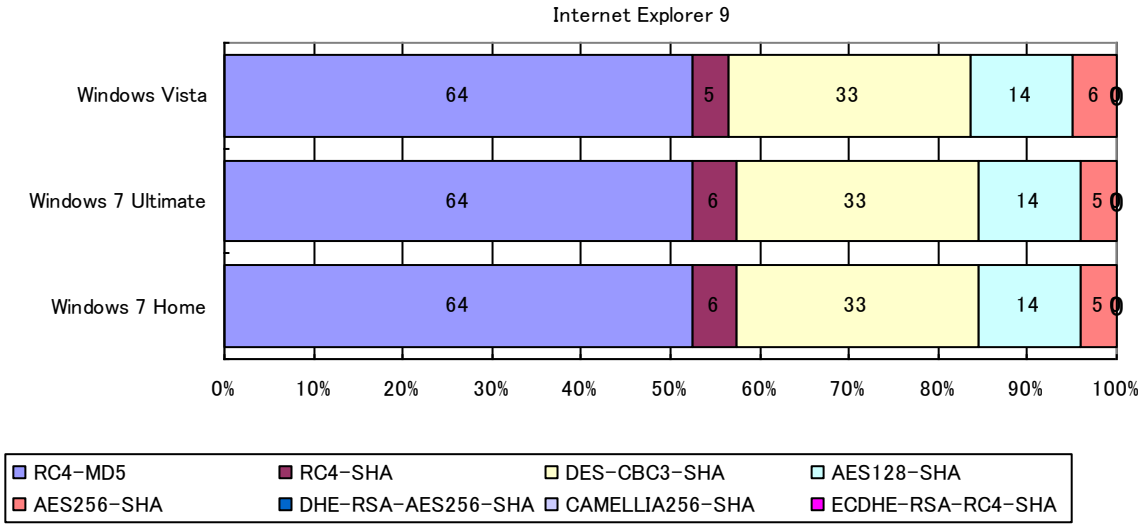
図表： Firefox 8 で接続に利用した Cipher suite <金融系：122 サーバ>



図表：Internet Explorer 7 で接続に利用した Cipher suite <金融系：122 サーバ>

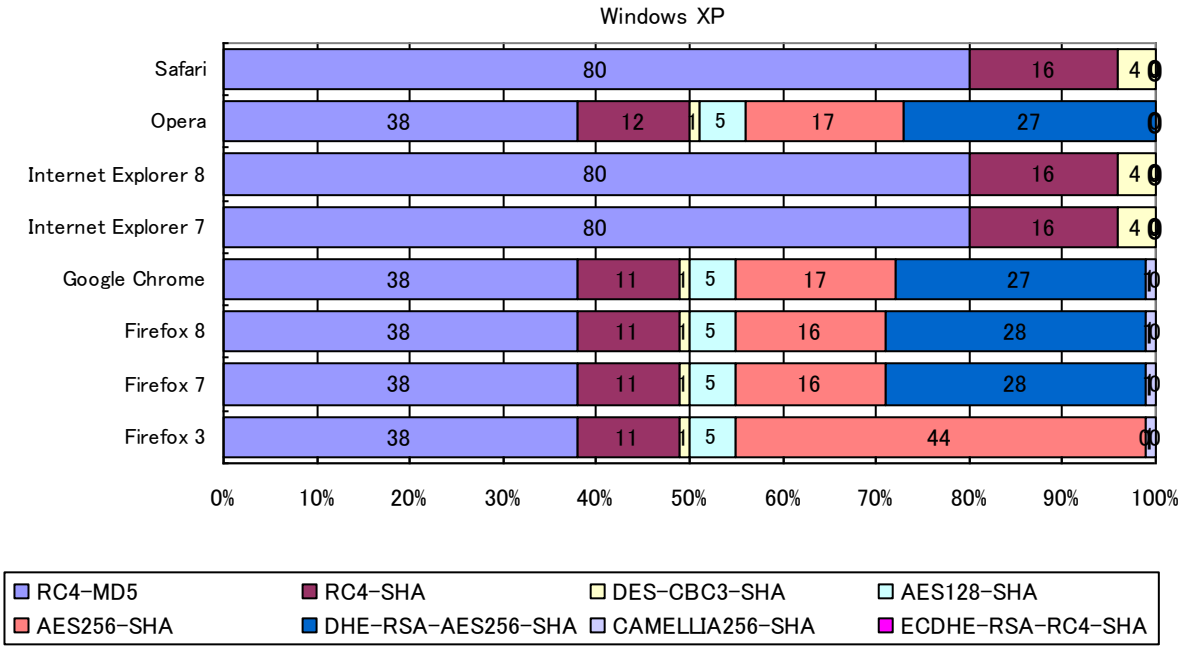


図表：Internet Explorer 8 で接続に利用した Cipher suite <金融系：122 サーバ>

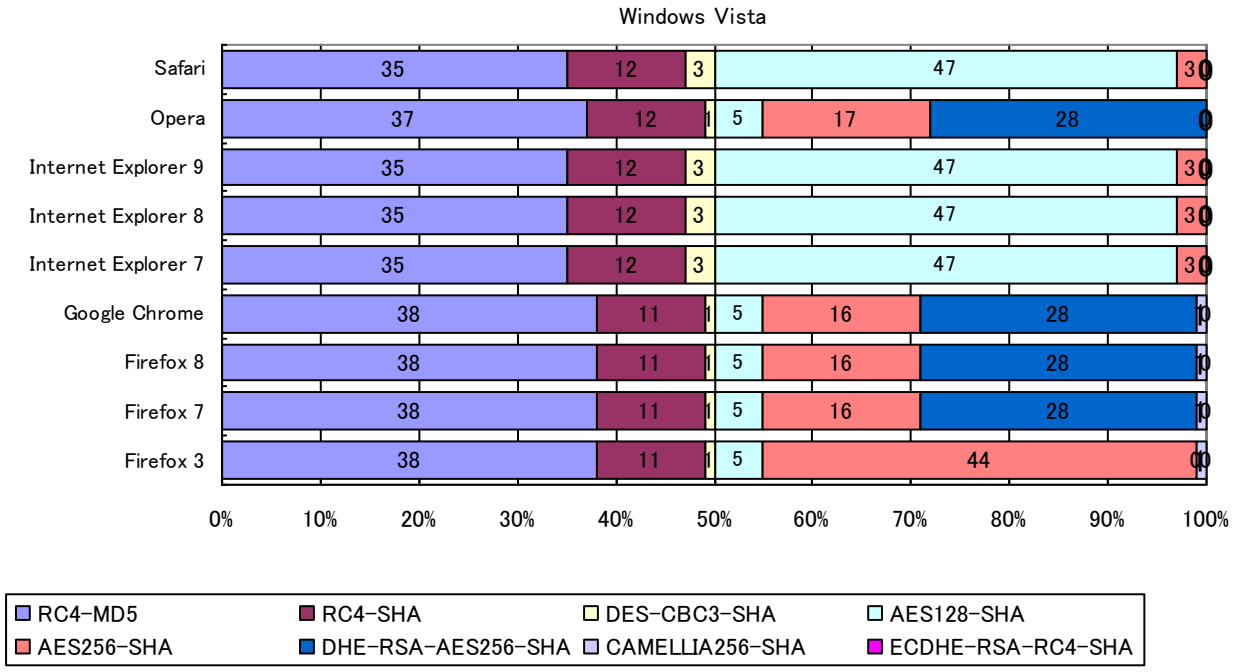


図表：Internet Explorer 9 で接続に利用した Cipher suite <金融系：122 サーバ>

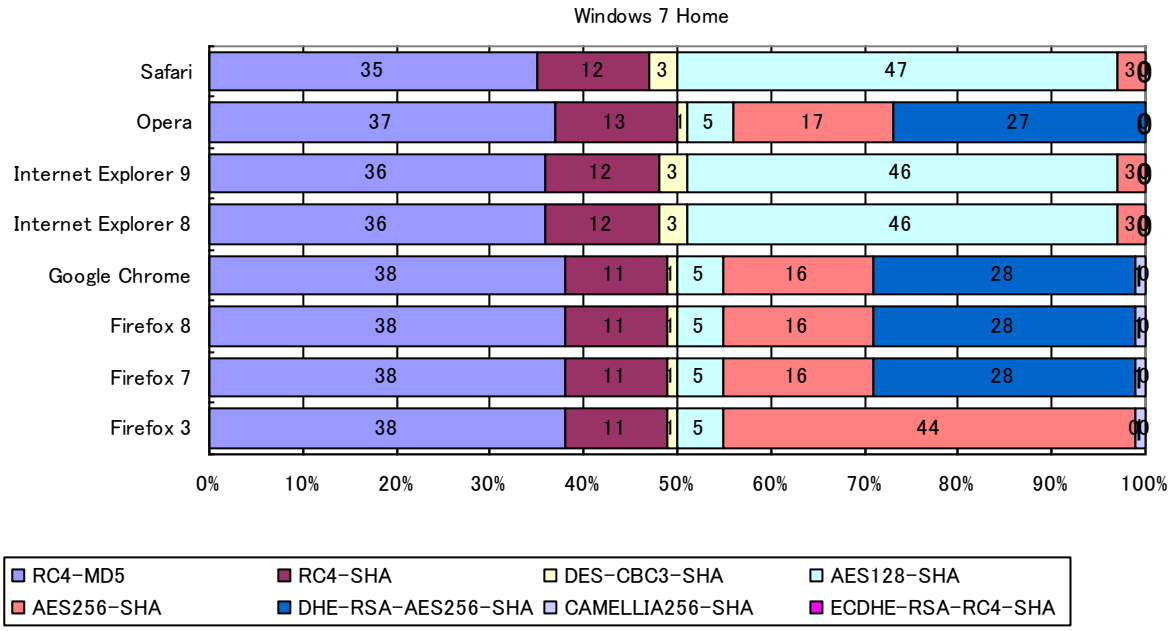
物販系詳細



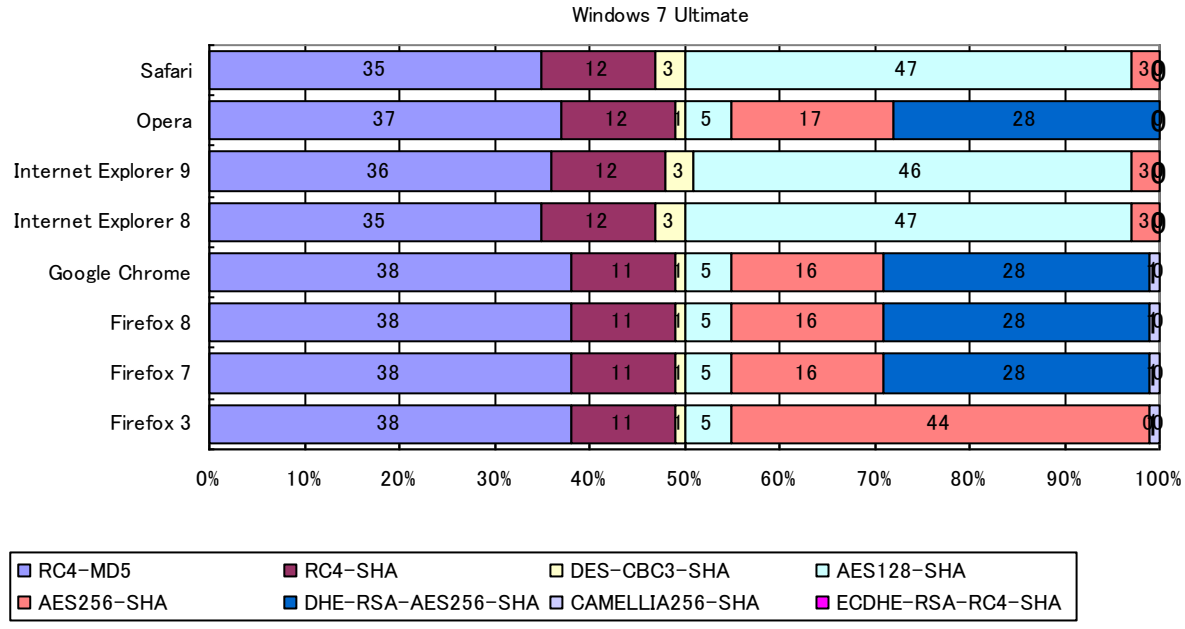
図表：Windows XP で接続に利用した Cipher suite <物販系：100 サーバ>



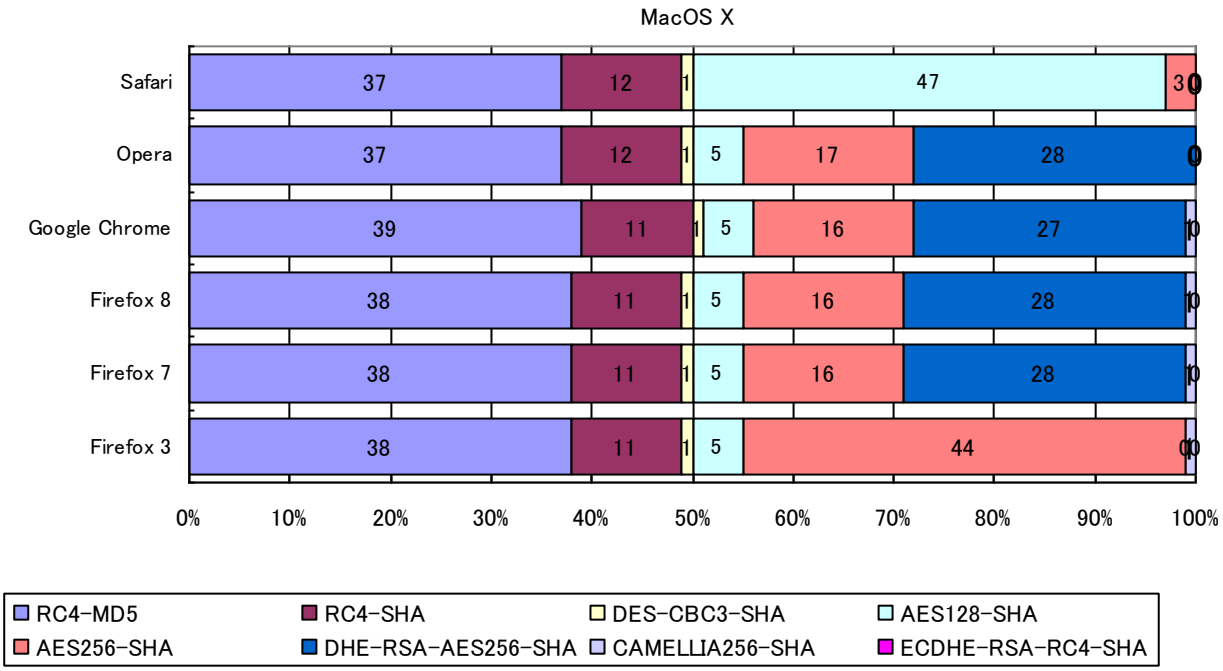
図表：Windows Vista で接続に利用した Cipher suite <物販系：100 サーバ>



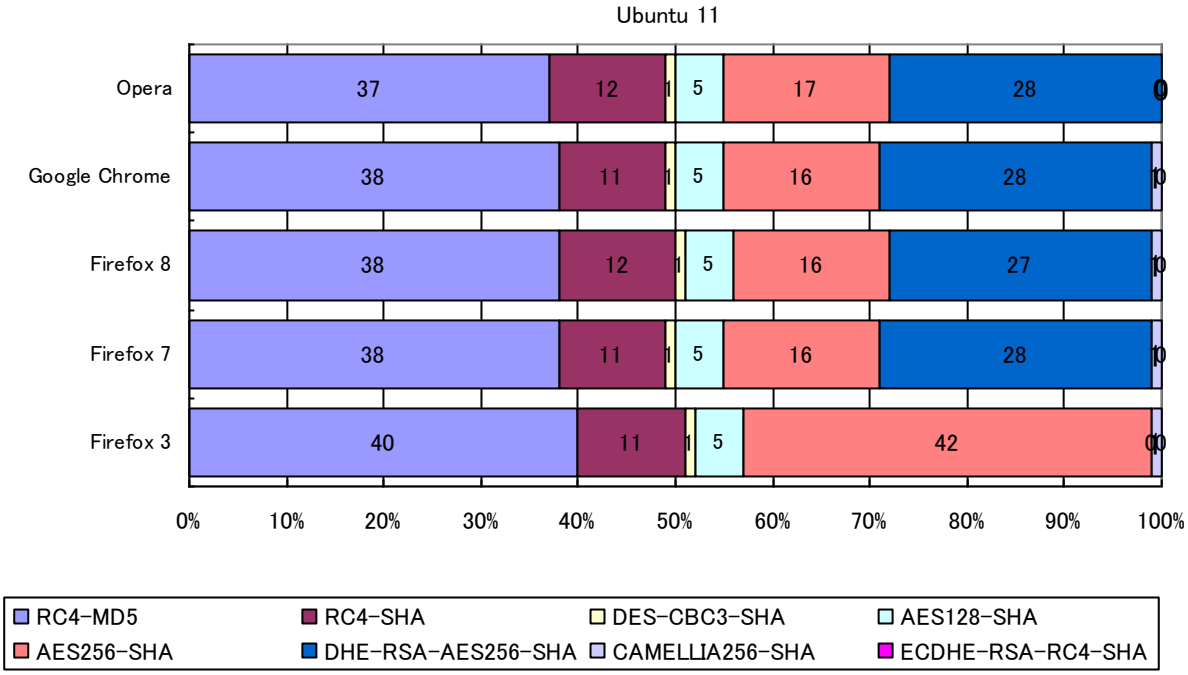
図表：Windows 7 Home で接続に利用した Cipher suite <物販系：100 サーバ>



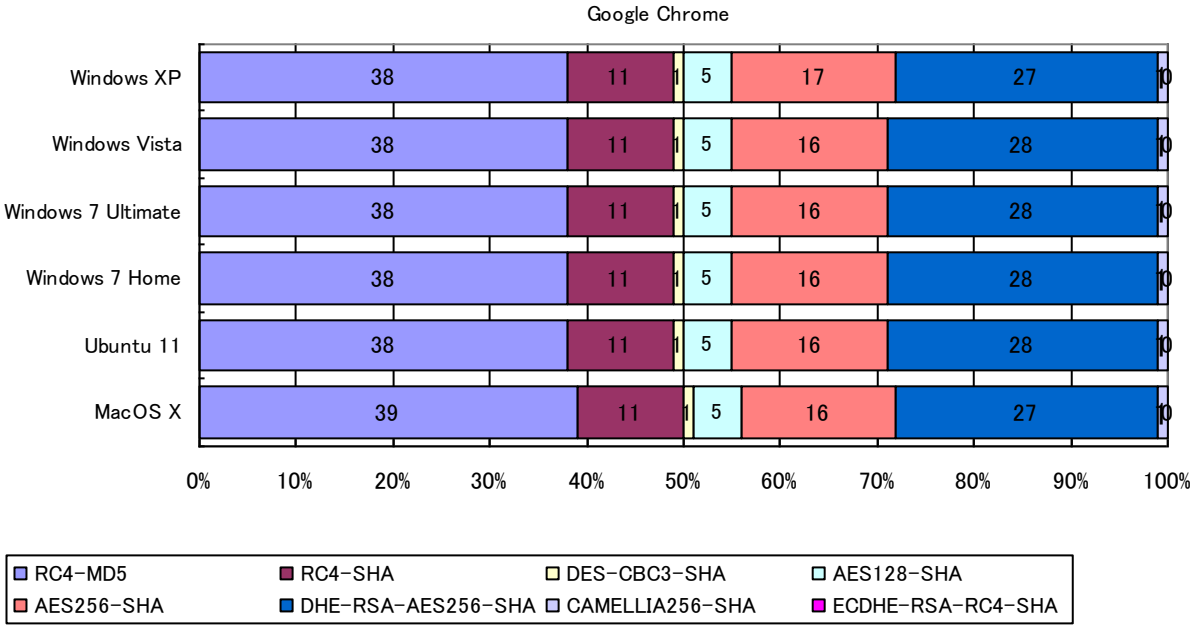
図表：Windows 7 Ultimate で接続に利用した Cipher suite <物販系：100 サーバ>



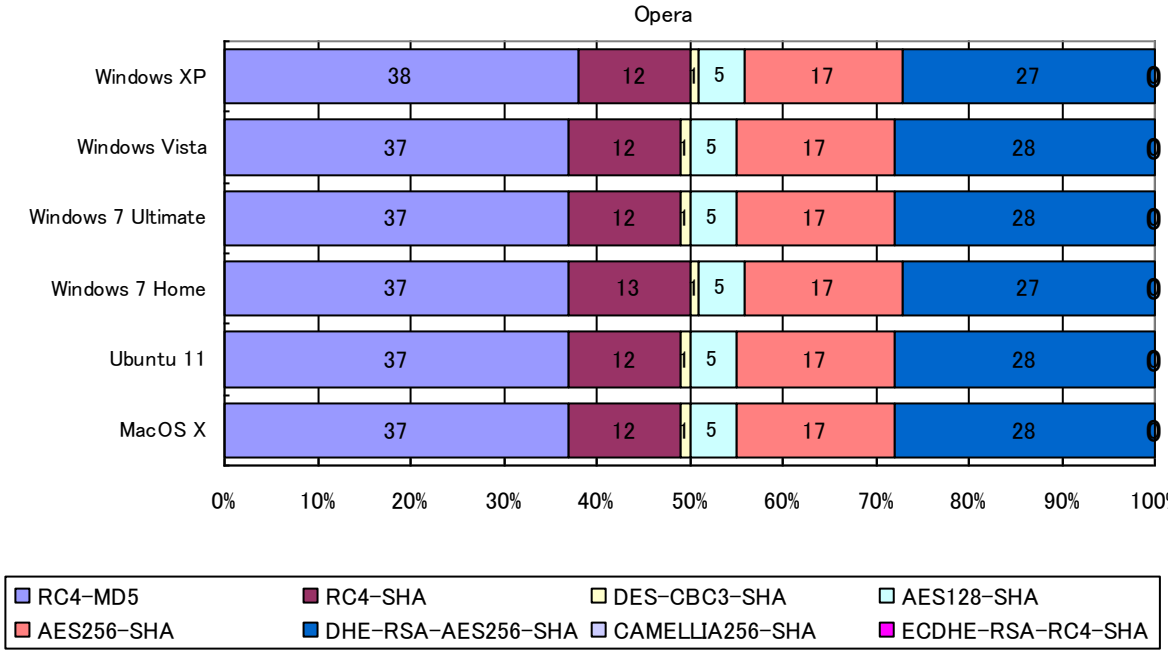
図表： MAC OS X **で接続に利用した** Cipher suite <**物販系：**100 **サーバ**>



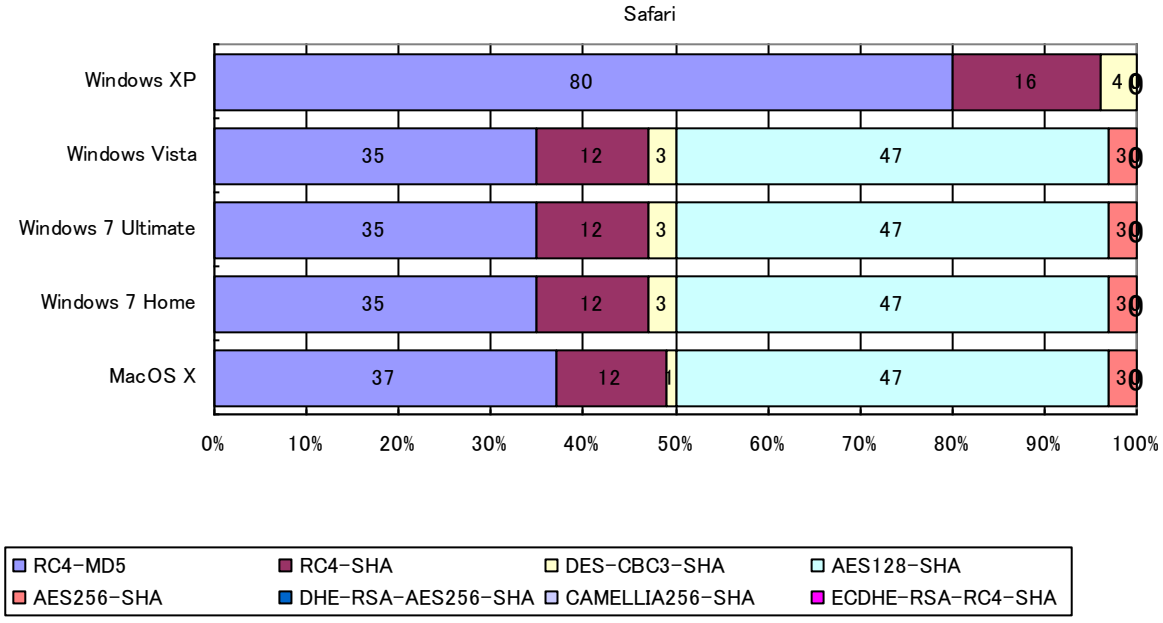
図表： Ubuntu 11 **で接続に利用した** Cipher suite <**物販系：**100 **サーバ**>



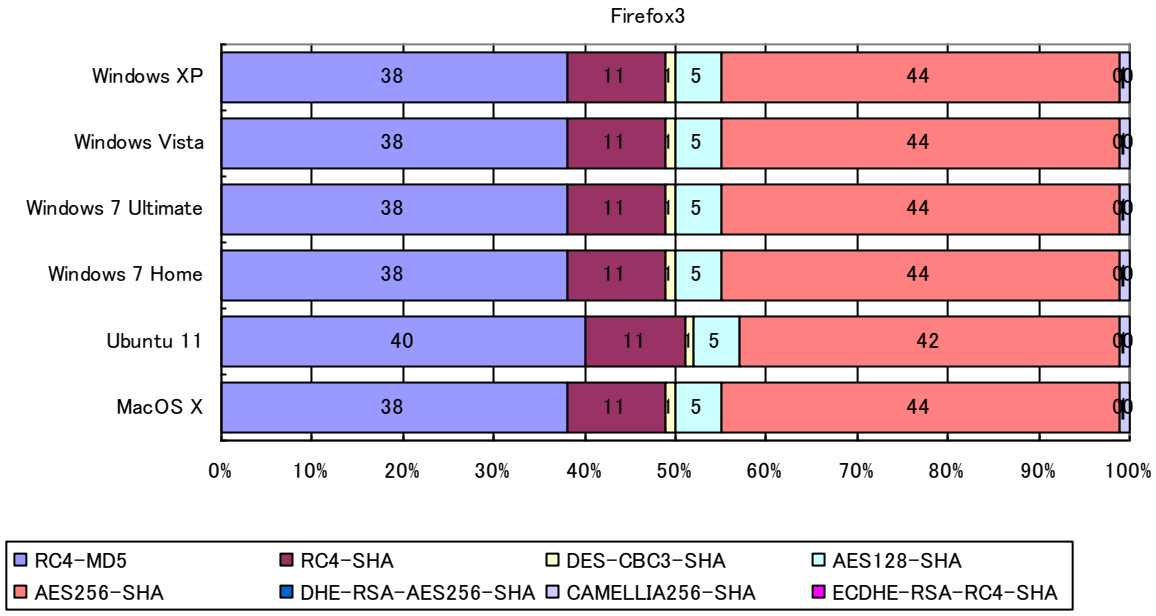
図表： Google Chrome **で接続に利用した** Cipher suite <**物販系：**100 **サーバ**>



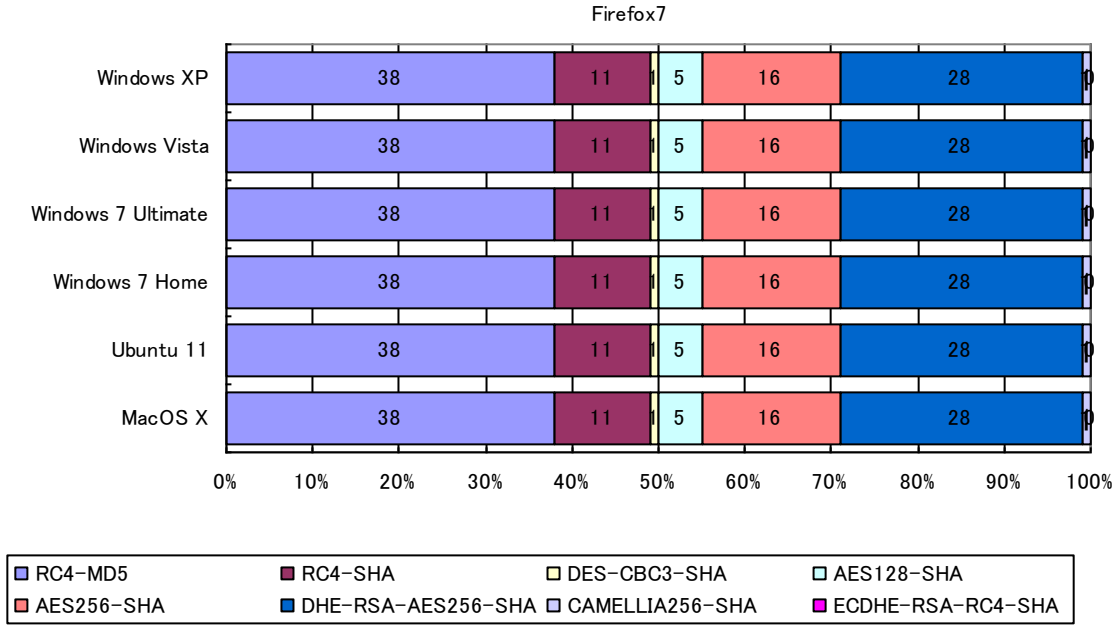
図表：Opera **で接続に利用した** Cipher suite <**物販系：**100 **サーバ**>



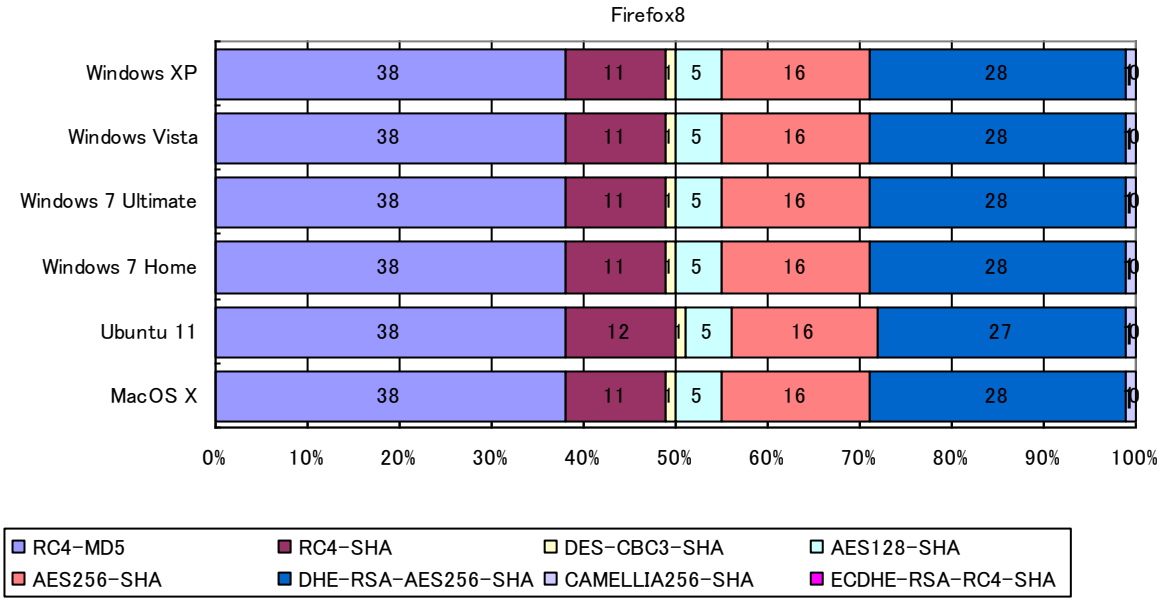
図表：Safari で接続に利用した Cipher suite <物販系：100 サーバ>



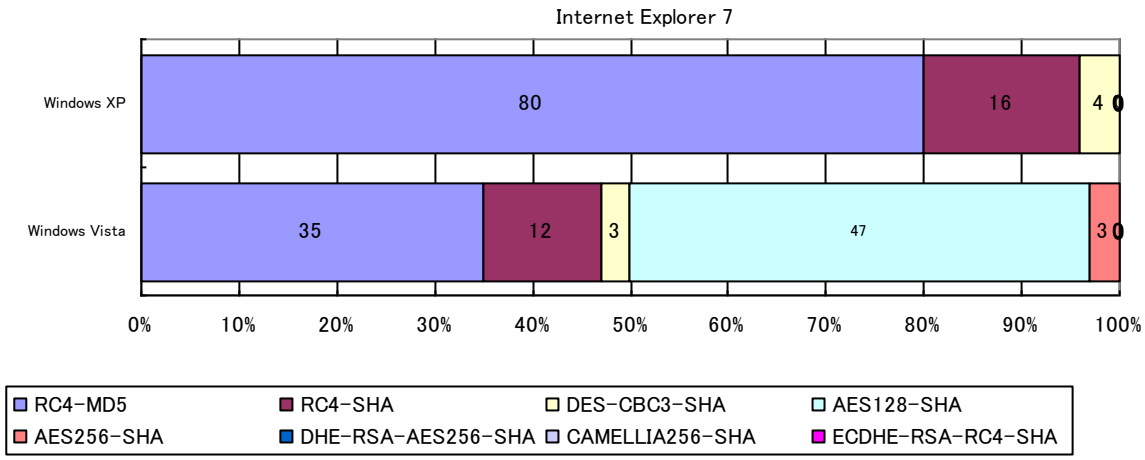
図表： Firefox 3 で接続に利用した Cipher suite <物販系：100 サーバ>



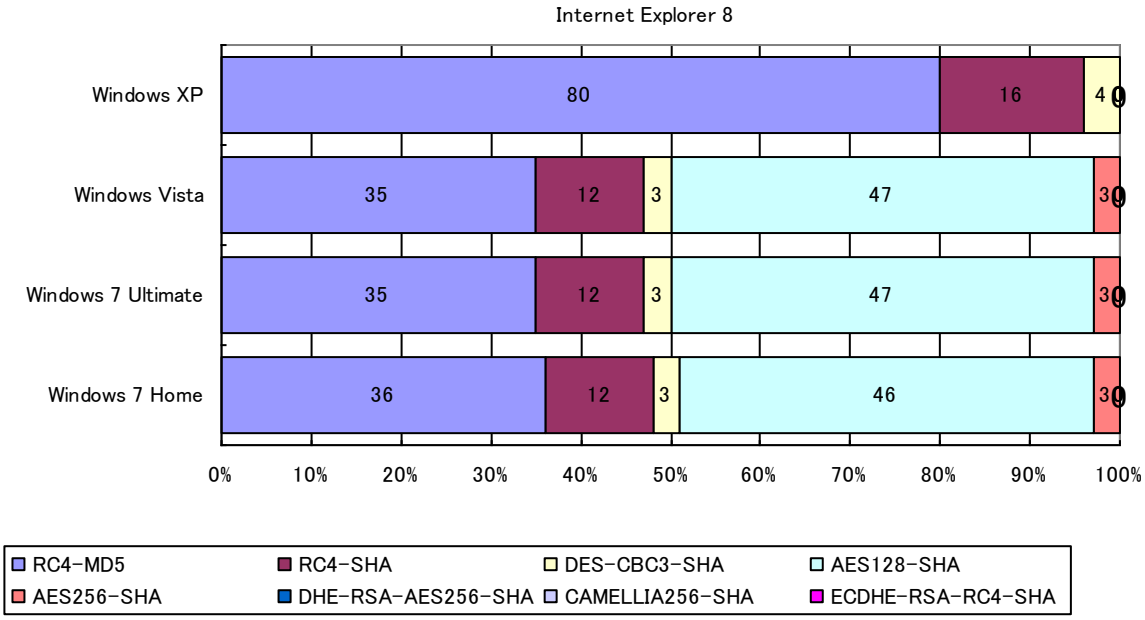
図表： Firefox 7 **で接続に利用した** Cipher suite <**物販系：**100 **サーバ**>



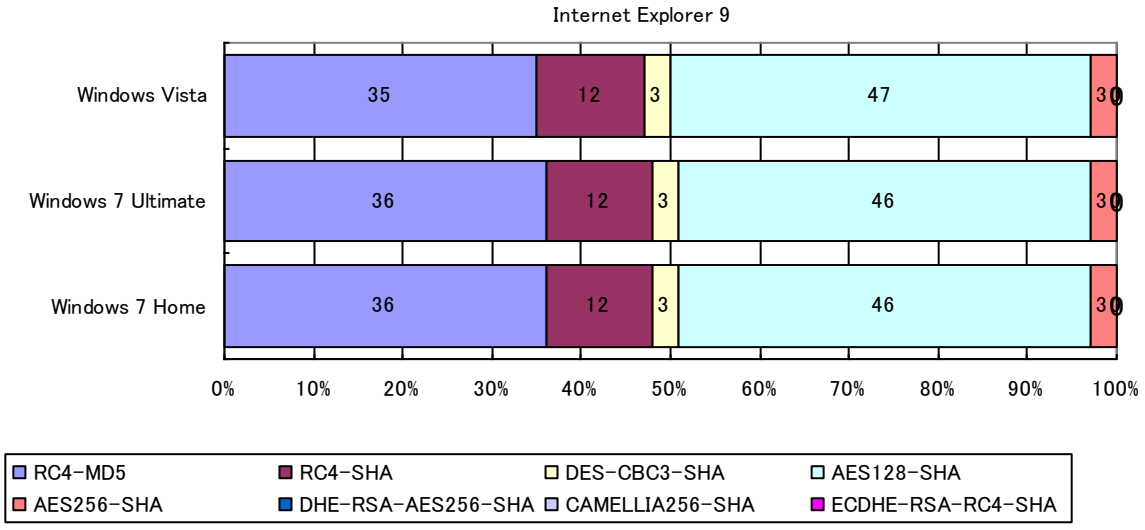
図表： Firefox 8 **で接続に利用した** Cipher suite <**物販系：**100 **サーバ**>



図表：Internet Explorer 7 で接続に利用した Cipher suite <物販系：100 サーバ>

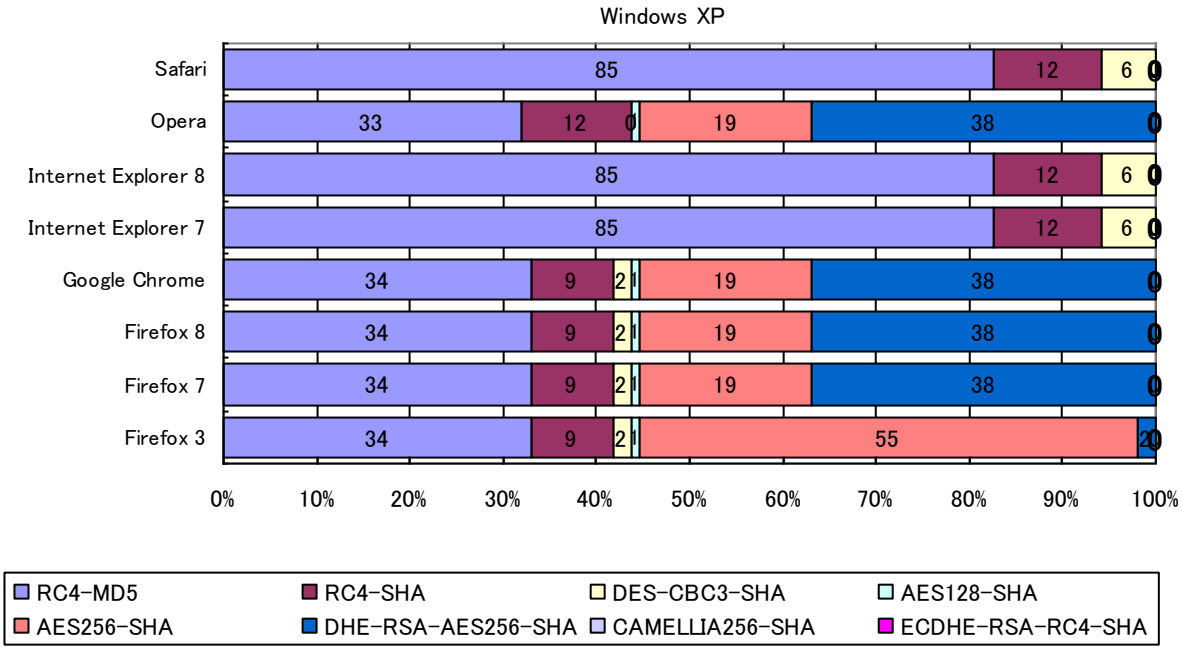


図表：Internet Explorer 8 で接続に利用した Cipher suite <物販系：100 サーバ>

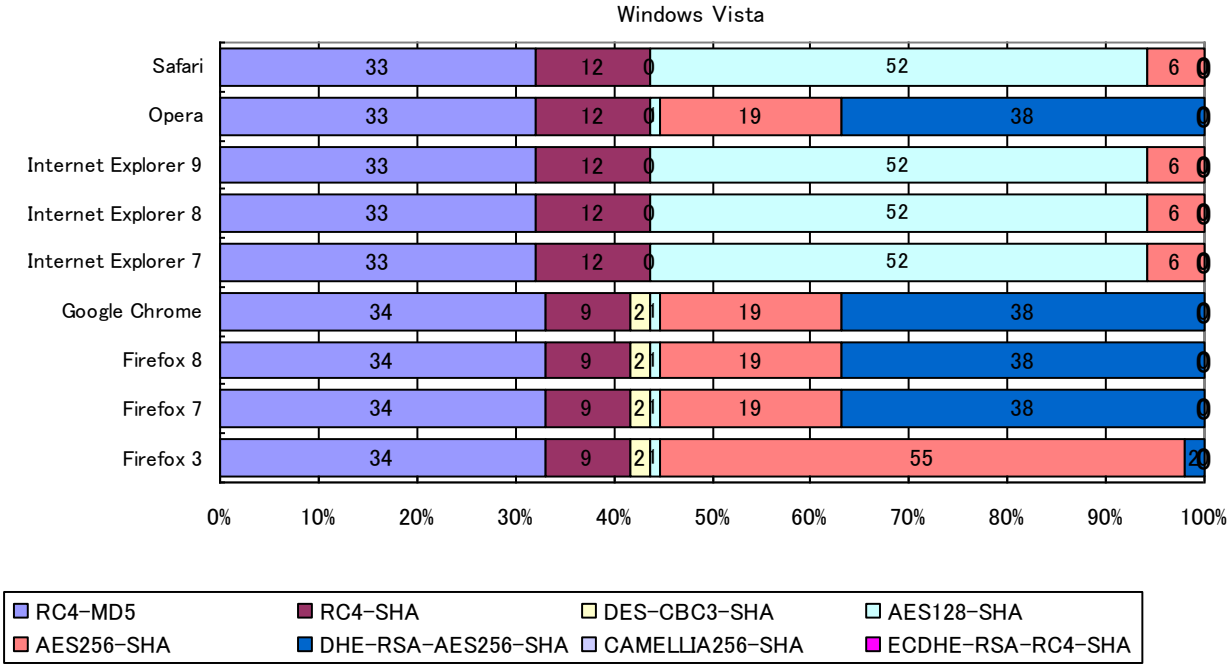


図表：Internet Explorer 9 で接続に利用した Cipher suite <物販系：100 サーバ>

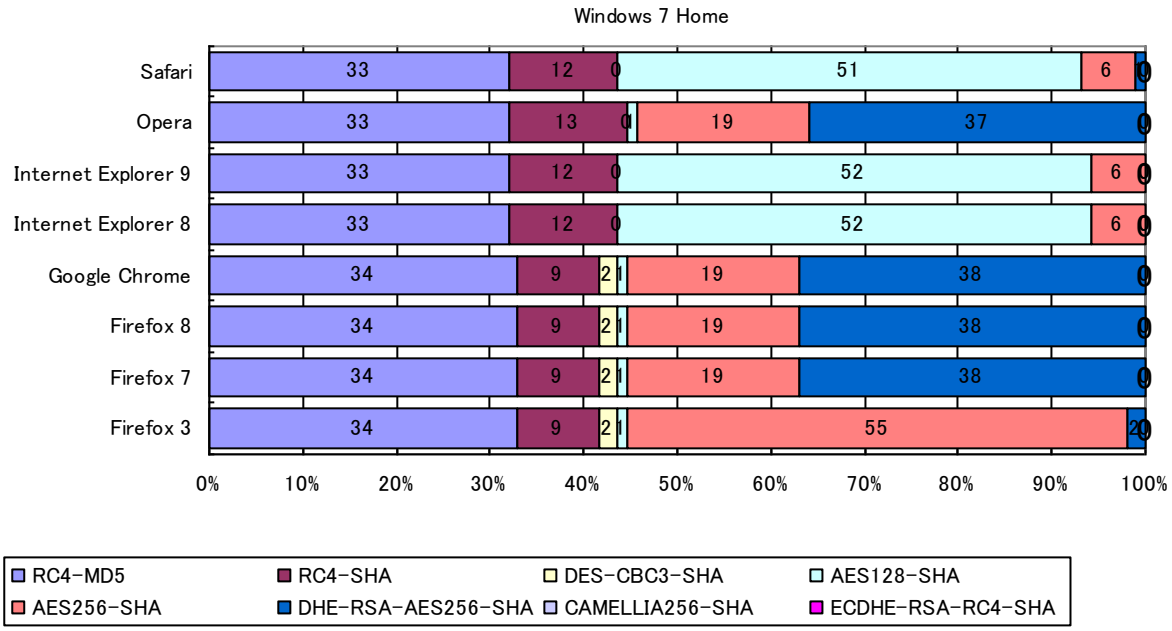
非物販系詳細



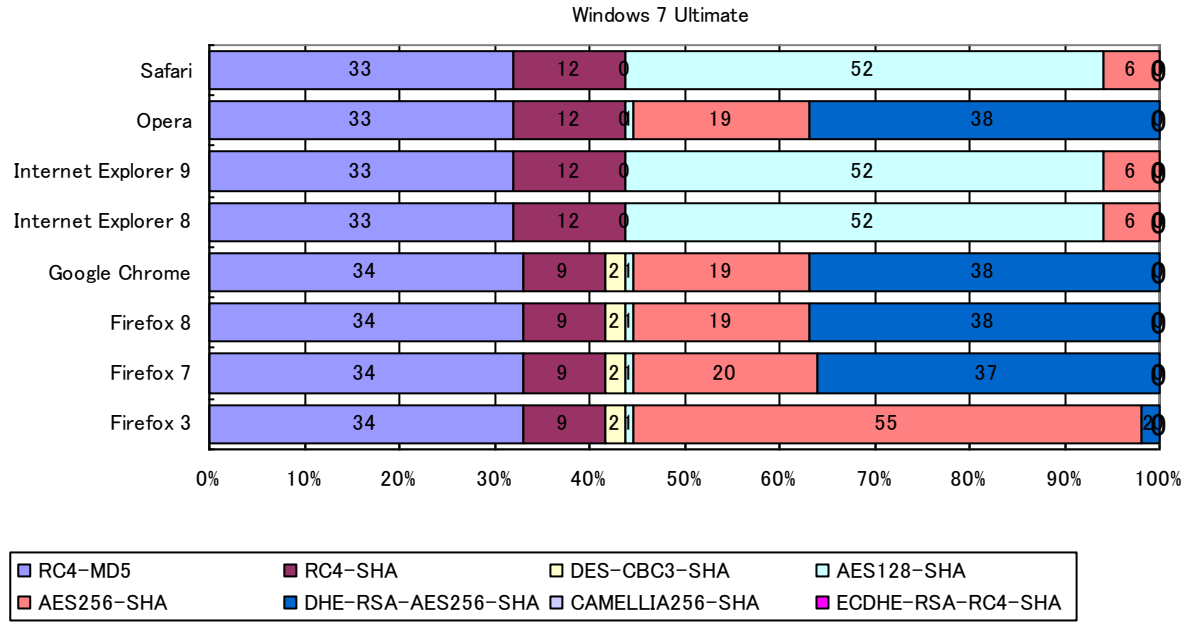
図表：Windows XP で接続に利用した Cipher suite <非物販系：103 サーバ>



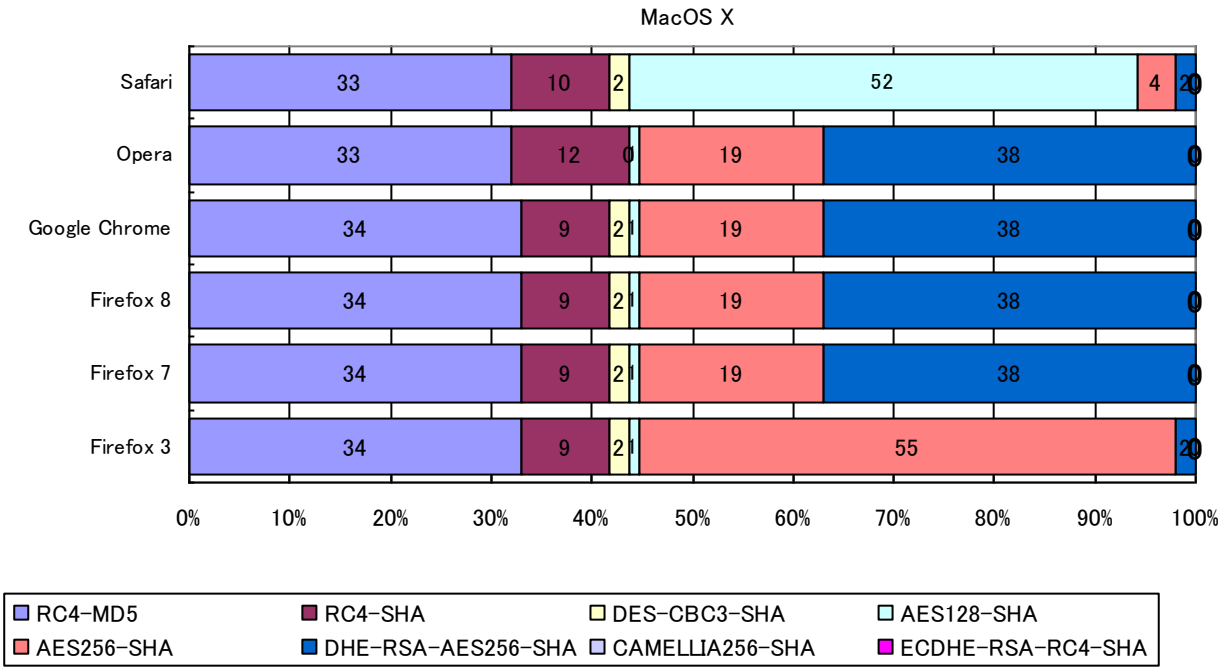
図表：Windows Vista で接続に利用した Cipher suite <非物販系：103 サーバ>



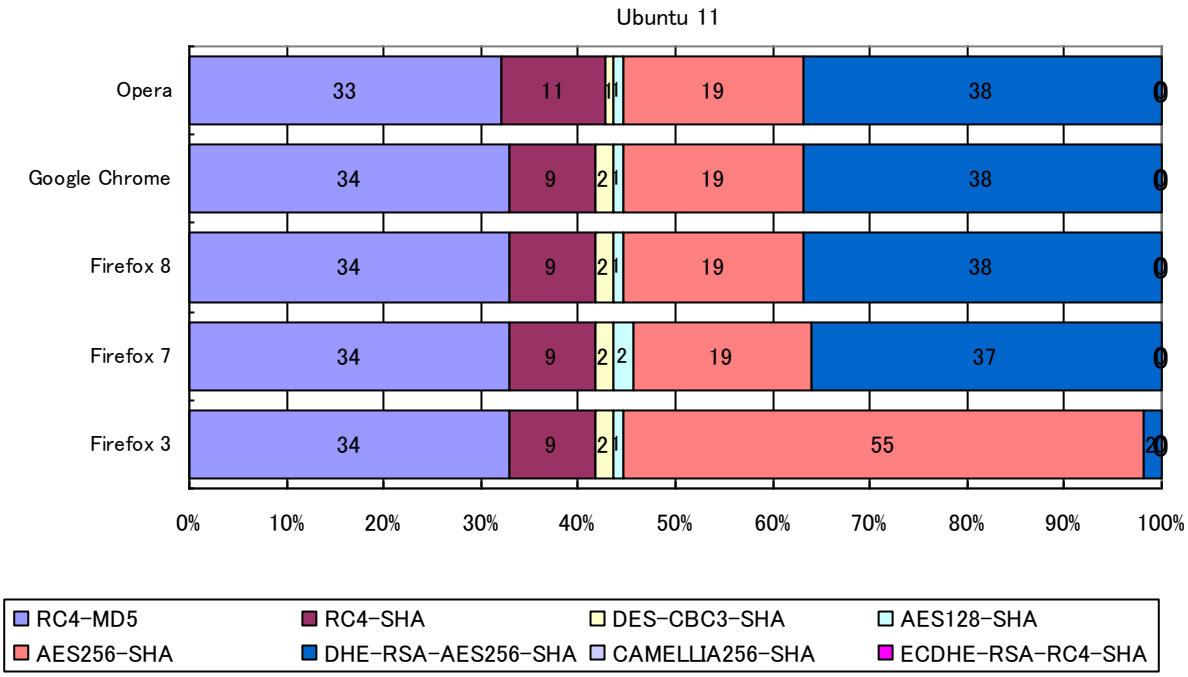
図表：Windows 7 Home **で接続に利用した** Cipher suite **<非物販系：103 サーバ>**



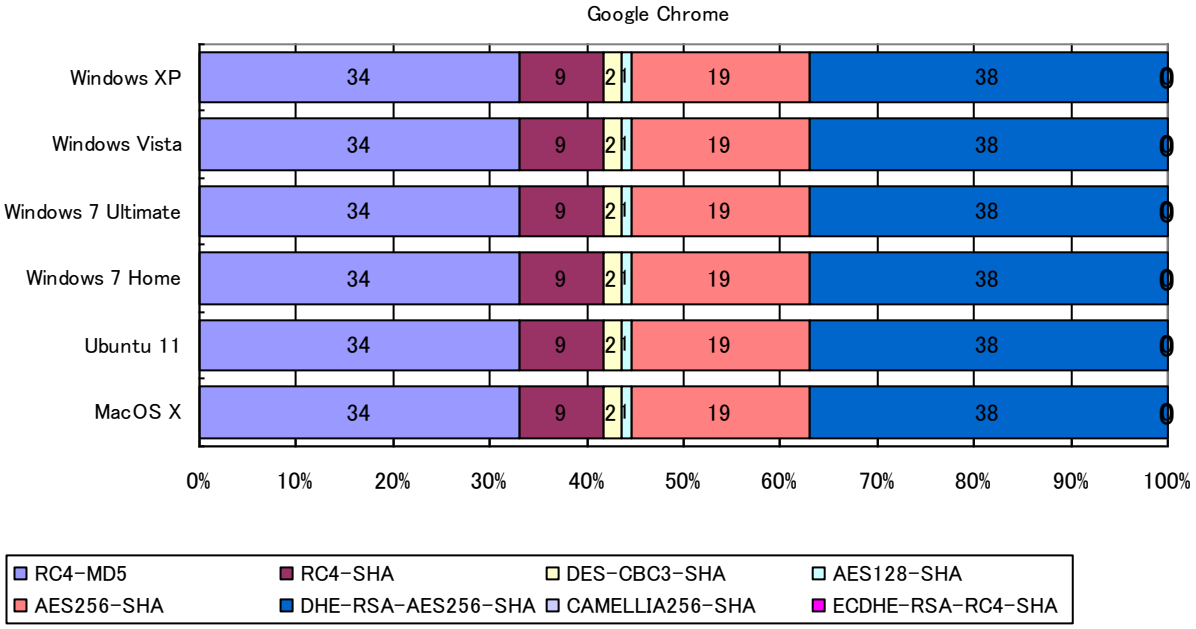
図表：Windows 7 Ultimate **で接続に利用した** Cipher suite **<非物販：103 サーバ>**



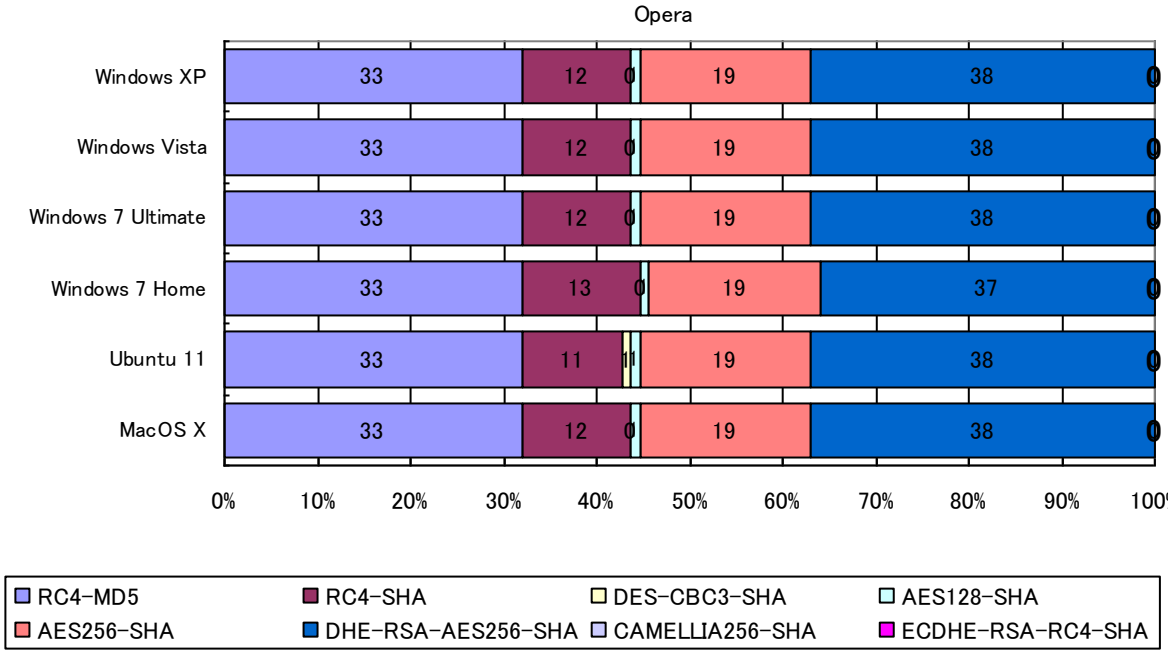
図表： MAC OS X **で接続に利用した** Cipher suite <**非物販系：**103 **サーバ**>



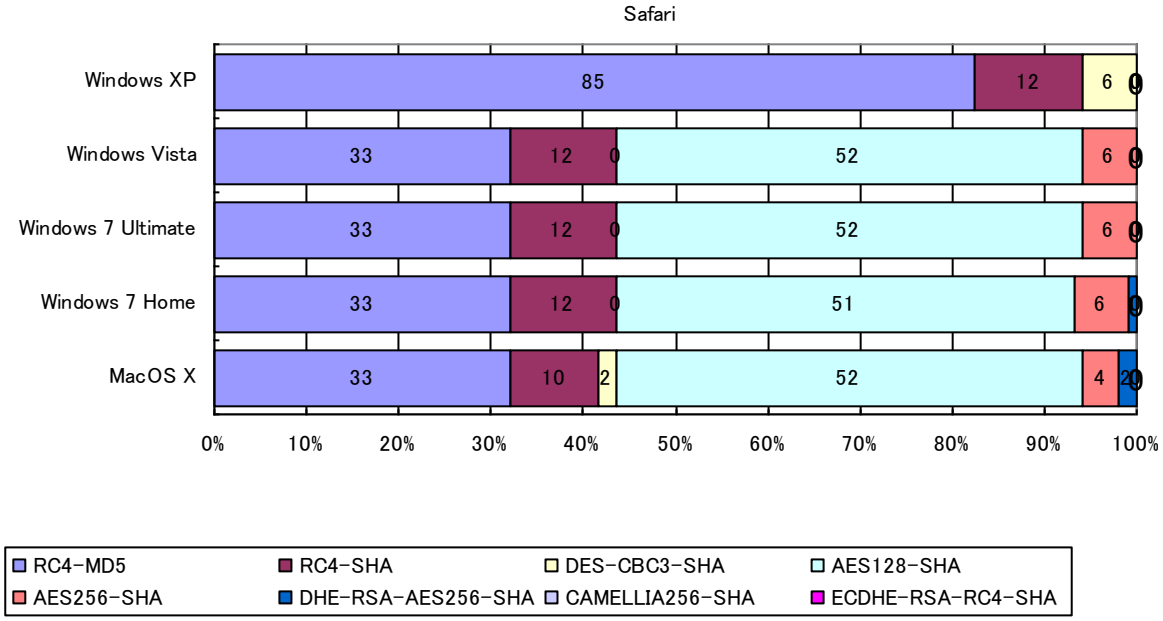
図表： Ubuntu 11 **で接続に利用した** Cipher suite <**非物販系：**103 **サーバ**>



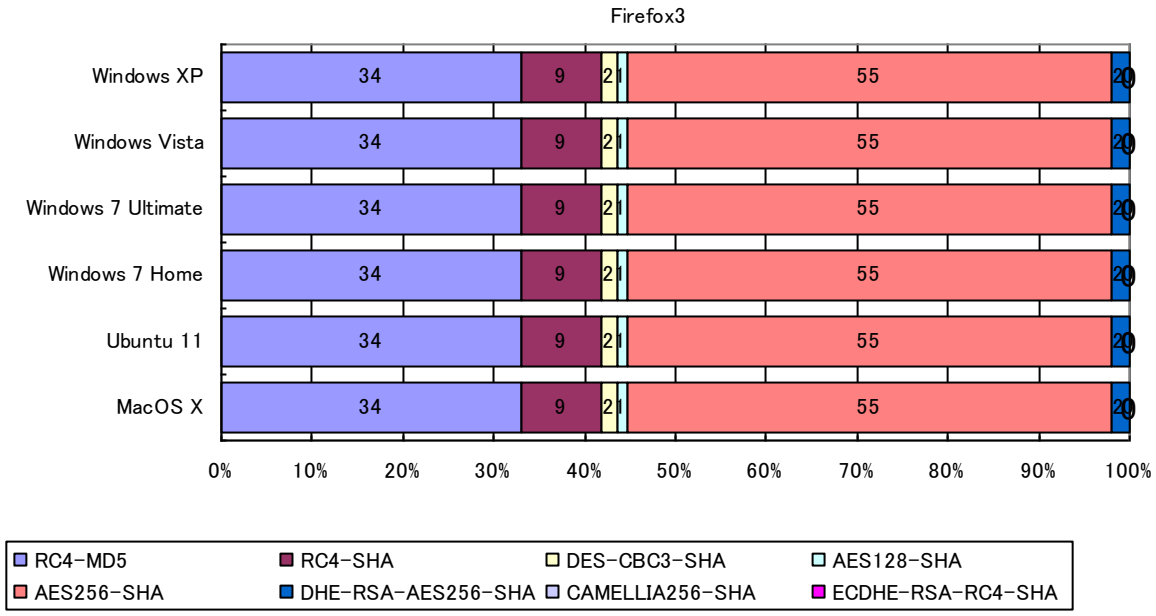
図表： Google Chrome **で接続に利用した** Cipher suite <**非物販系：**103 **サーバ**>



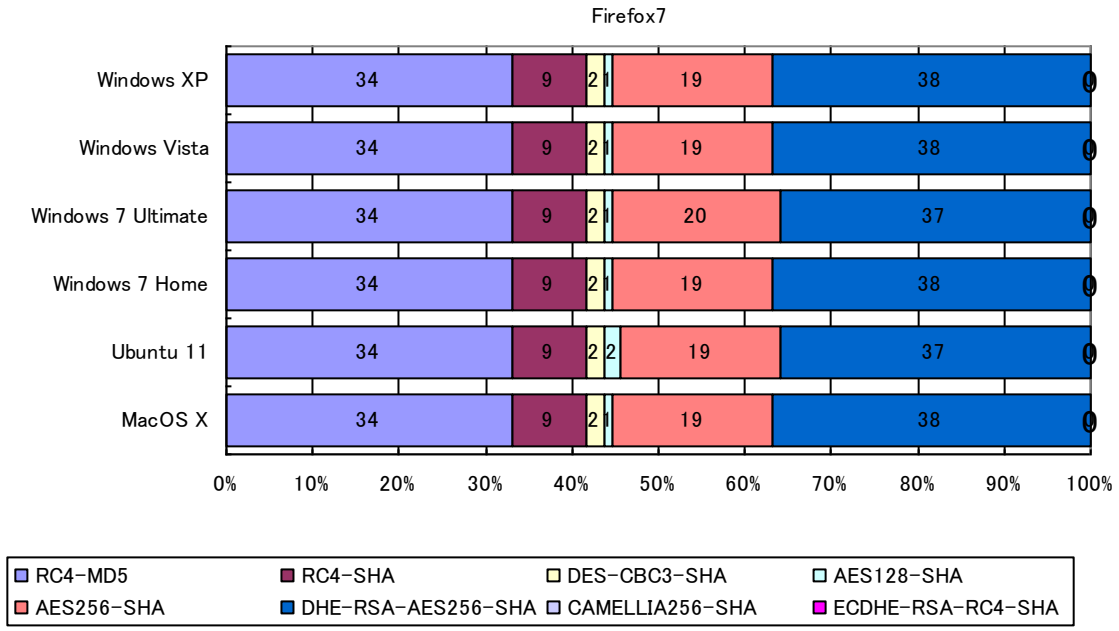
図表：Opera **で接続に利用した** Cipher suite <**非物販系：**103 **サーバ**>



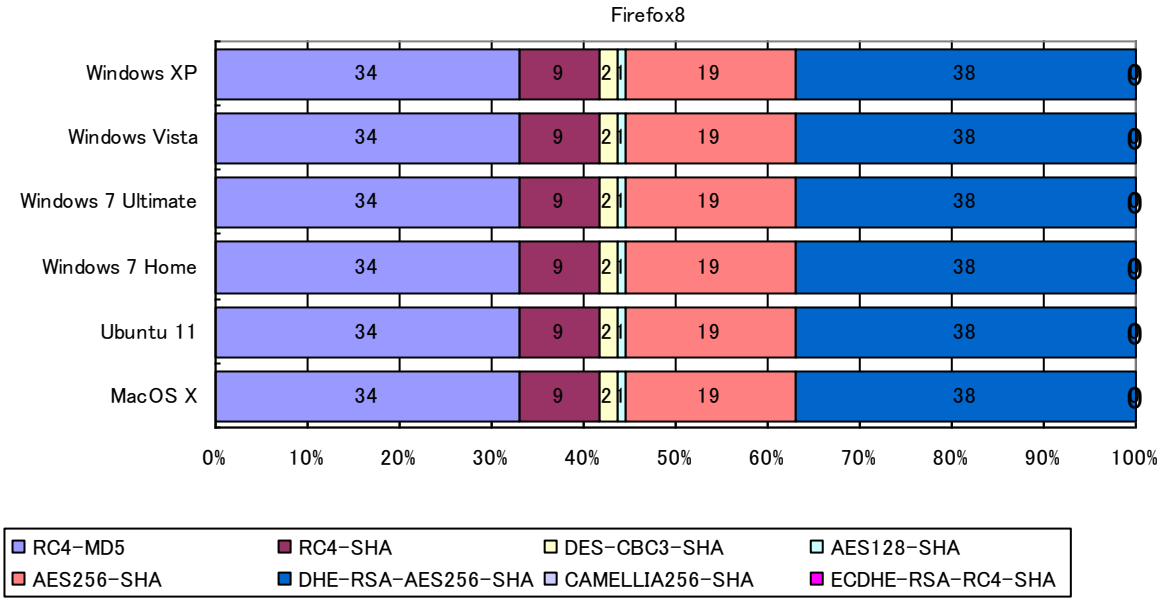
図表：Safari で接続に利用した Cipher suite <非物販系：103 サーバ>



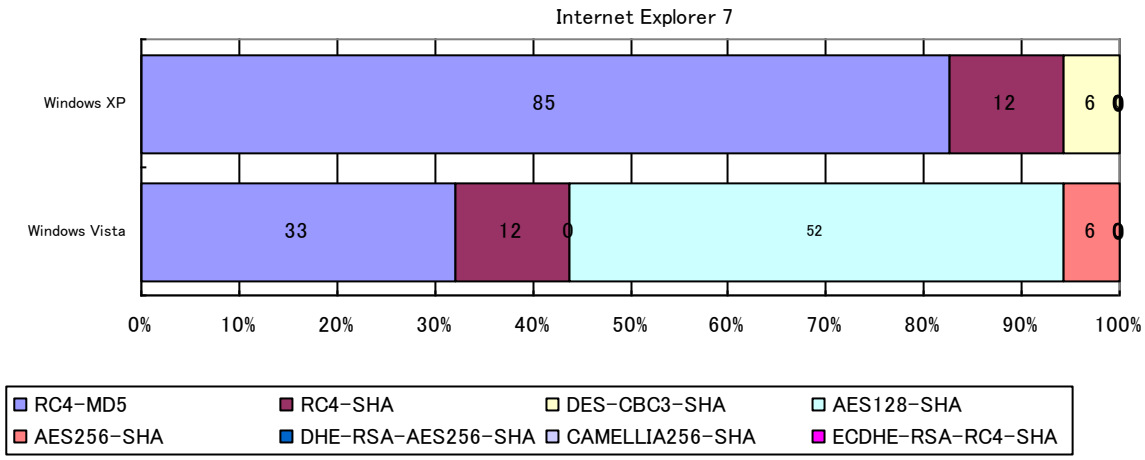
図表： Firefox 3 で接続に利用した Cipher suite <非物販系：103 サーバ>



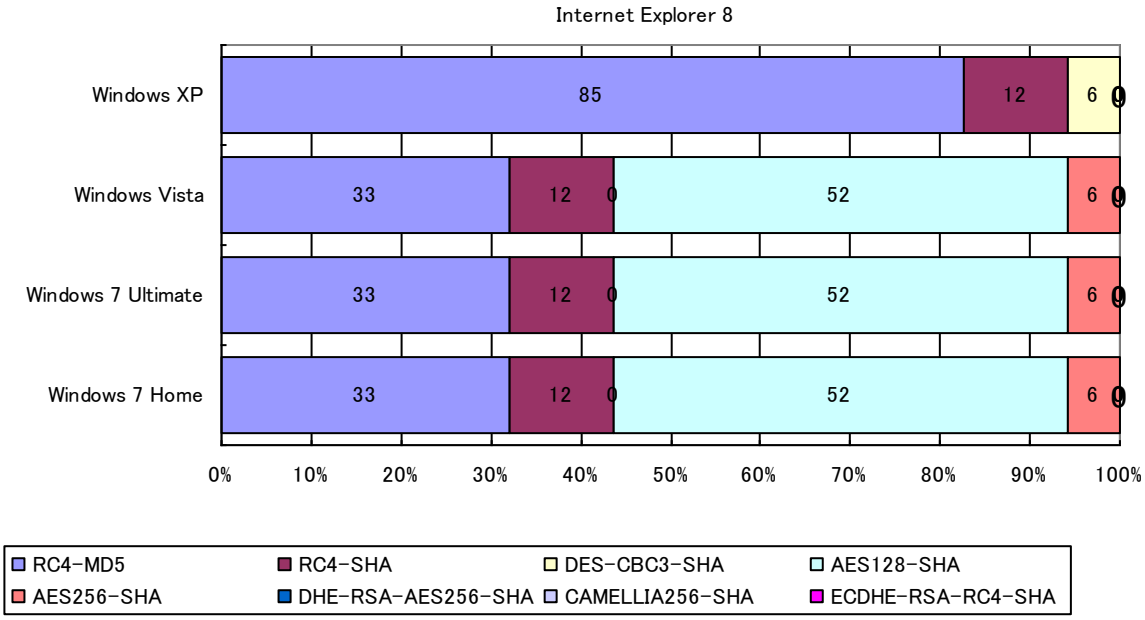
図表： Firefox 7 **で接続に利用した** Cipher suite <**非物販系：**103 **サーバ**>



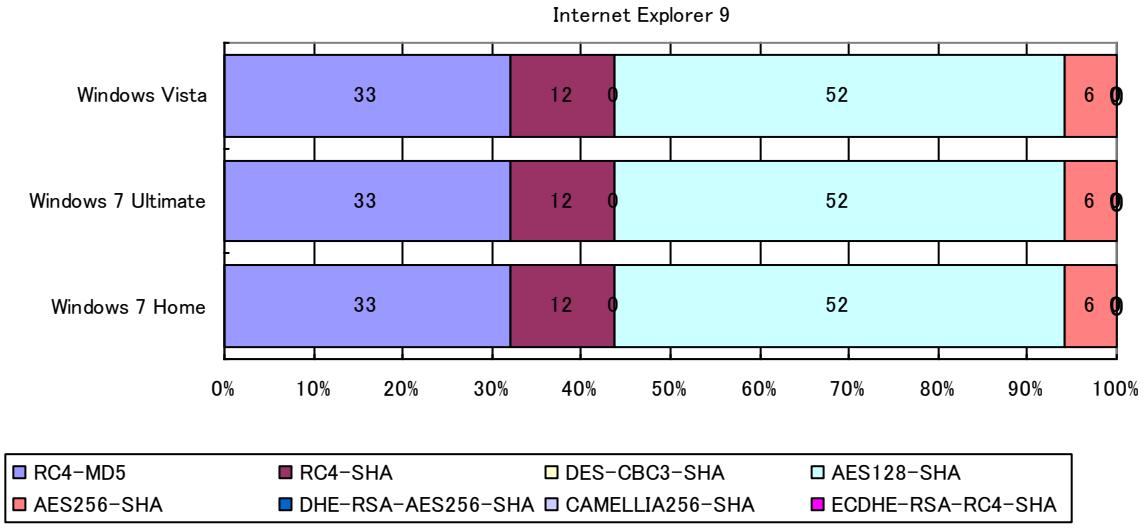
図表： Firefox 8 **で接続に利用した** Cipher suite <**非物販系：**103 **サーバ**>



図表：Internet Explorer 7 で接続に利用した Cipher suite <非物販系：103 サーバ>



図表：Internet Explorer 8 で接続に利用した Cipher suite <非物販系：103 サーバ>



図表：Internet Explorer 9 で接続に利用した Cipher suite <非物販系：103 サーバ>

7. 付録一覧

１．　ＳＳＬデフォルト設定調査結果　～サーバ編～
２．　ＳＳＬデフォルト設定調査結果　～クライアント編～

別紙調査シート

調査対象ＳＳＬサーバ（金融系）リスト
調査対象ＳＳＬサーバ（物販系）リスト
調査対象ＳＳＬサーバ（非物販系）リスト
接続可能な Cipher suite 調査結果　（金融系）
接続可能な Cipher suite 調査結果　（物販系）
接続可能な Cipher suite 調査結果　（非物販系）
クライアント環境における Cipher suite 調査結果　（金融系）
クライアント環境における Cipher suite 調査結果　（物販系）
クライアント環境における Cipher suite 調査結果　（非物販系）
スマートフォン環境における Cipher suite 調査結果

余白