4L クラウドセキュリティアライアンスとその活動について

勝見　勉　（独）情報処理推進機構

クラウドセキュリティアライアンスはクラウドコンピューティングのセキュリティのためのベストプラクティスの普及を目指す団体で，2009 年 4 月発表のクラウドセキュリティガイダンス（Security Guidance for Critical Areas of Cloud Computing）は世界的注目を集めた．その後も各種レポートの発行や世界各地での講演等精力的に活動を展開し，クラウドコンピューティングのセキュリティ研究において一つの極を形成している．日本では日本支部を設立し，また情報処理推進機構とは相互協力協定を締結して活動の幅を広げている．本稿では，その活動の概要を紹介し，クラウドセキュリティガイダンスを日本で適用する場合の解釈や実装の指針の開発等，今後の課題について概観する．

クラウドセキュリティアライアンスとは

クラウドセキュリティアライアンス（Cloud Security Alliance，略称 CSA）は，アメリカ・ワシントン州に本拠を置く非営利法人で，国際的活動を行っている．本拠といってもバーチャルなもので，活動の実態は個別のプロジェクトが世界のさまざまなところで，物理的に，あるいはバーチャルに行われるかたちとなっている．そのコミュニケーションの手段は，LinkedIn（リンクトイン）というソーシャルネットワーキングサービスが中心となり，それに案件ごと，プロジェクトごとの電子メールまたは電話会議が加わって，いずれもバーチャルな世界で展開されている．

その目的は，CSA の Web ページにあるミッションステートメントによれば「クラウドコンピューティングのセキュリティ保証のためのベストプラクティスの普及を目指すとともに，クラウドコンピューティングのユーザへの教育を通じてあらゆるコンピューティング形態を安全にする」こととしている．そして，その専門能力に長けた多様な構成メンバを背景に，次の活動を行うとしている（日本語訳は筆者）．

1）クラウドコンピューティングに必要なセキュリティ要件とその保証のための検証について，プロバイダ側，ユーザ側共通のレベルの理解の形成を促進すること
2）クラウドコンピューティングのベストプラクティスについての独自の研究の推進
3）クラウドコンピューティングの適切な利用とクラウドセキュリティのソリューションについての啓発キャンペーンと教育プログラムの実施
4）クラウドのセキュリティ保証に関する共通課題リストとガイダンスの開発

CSA は会員制度をとっている．連携会員（Affiliate Members），法人会員（Corporate Members），個人会員（Individual Members）の区分がある．会費負担があるのは法人会員だけで，年会費は 1 万米ドルに設定されている．連携会員は非営利団体もしくは業界団体で，特定のテーマで相互協力の約束を交わした団体が登録されている．2010 年 8 月 20 日現在，世界中で 14 団体がリストされている．政府系では，筆者が所属する日本の（独）情報処理推進機構（IPA）と EU の ENISA（欧州ネットワーク情報セキュリティ庁）がある．ほかには OWASP[☆1]

☆1 OWASP : Open Web Application Security Project．アプリケーションソフトウェアのセキュリティ向上を目指す非営利のグローバルな活動団体．http://www.owasp.org/index.php/Main_Page

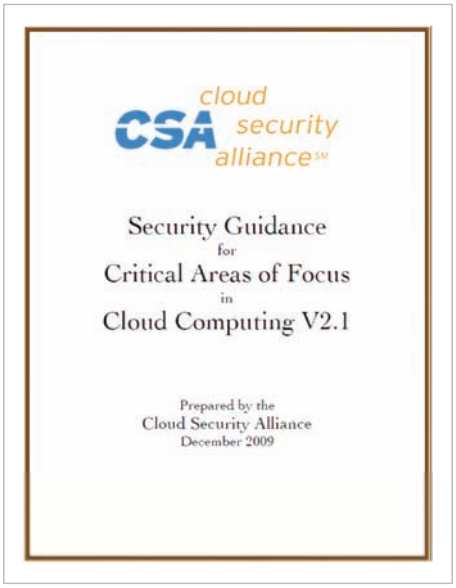

図-1 クラウドセキュリティガイダンスの表紙

や DMTF[☆2] といった標準化団体も名を連ねている．法人会員は 54 社を数える．クラウドベンダは Google，Microsoft 以外は 3Par，RackSpace，TerreMark，ZScaler などあまり規模の大きくない企業で，数もさほど多くない．逆にセキュリティベンダは多く，TrendMicro をはじめ，Symantec，McAfee，RSA Security，Qualys などの大手が名を連ねる．また HP，Dell，AT&T，CA，Cisco，Oracle，Novell，IBM といった IT 大手が数多く参加している．日本からは法人会員は入っていない．一方，中国からは Lenovo，NSFocus，瑞星が，インドからは Tata Communications が参加している．両国の勢いを見る思いがする．

CSA の運営は，主に法人会員の会費によって賄われている．個人会員は現在全世界で 1 万人を超えていると見られる．特に資格要件もなく，会費負担もない．唯一の条件は LinkedIn で CSA のグループメンバになることである．CSA のグループへの参加承認依頼をあげるだけで，ほぼ自動的に参加承認される．このようにして，個人会員は日々増え続けている．

CSA の設立日はあまり明確にされていない．その経緯説明によれば，創設者で Executive Director を務める Jim Reavis が，2008 年 11 月 20 日に ISSA[☆3] の CISO フォーラムでクラウドのセキュリティについて講演したのがきっかけとなり，クラウドのセキュリティのための団体の必要性に賛成する人たちにより，その年の 12 月に発足したと述べられている．創設メンバとしては Nils Puhlmann，Dave Cullinane，Philippe Courtot，Alan Boehme，Izak Mutlu，Jay Chaudhry，Christofer Hoff，Paul Kurtz，Jean Pawluk がいる．そもそもの発端がこのような人的つながりを出発点としているため，CSA は今でもヒューマンリレーションズをベースとする活動の色彩を強く残している．

クラウドセキュリティアライアンスの活動の概要

CSA では，いくつかのワークグループや SIG（Special Interest Group）が編成され活動している．その活動成果は，時々 CSA のアウトプットとして公表される．以下に，いくつかのアウトプットと，現在進行中の活動を紹介する．

(A) クラウドセキュリティガイダンス

英語のフル名称は Security Guidance for Critical Areas of Focus in Cloud Computing という長い名前である（図-1）．2009 年 4 月，RSA カンファレンスの中で Version 1 が発表され，世界的に注目を集めた[☆4]．クラウドコンピューティングのセキュリティ課題について 3 分野 15 領域にわたって課題を抽出し，その内容と対策を記述している．取り上げられた項目のリストは以下の通りである（日本語訳は筆者）．

1. クラウドアーキテクチャ分野
   ①クラウドコンピューティングのアーキテクチャフレームワーク

☆2 DMTF : Distributed Management Task Force．IT システム管理の相互運用性を達成するための標準化開発を推進する団体．http://www.dmtf.org/
☆3 ISSA : Information Systems Security Association．情報セキュリティの専門家と実践者による非営利のグローバルな活動団体．https://www.issa.org/
☆4 このガイダンスはその後，2009 年 12 月には改訂版（Version 2.1）が発行されている．なお，Version 1 は日本語訳が行われ，インプレス社から発刊されている．

2. クラウドのガバナンス分野
　②ガバナンスとエンタープライズリスク管理
　③法的問題
　④電子的証拠開示
　⑤コンプライアンスと監査
　⑥情報ライフサイクル管理
　⑦移植性と相互運用性
3. クラウドの運用分野
　⑧従来からのセキュリティ，事業継続，災害復旧
　⑨データセンタの運用
　⑩インシデント対応，通知，対策アプリケーションのセキュリティ
　⑪アプリケーションセキュリティ
　⑫暗号化と鍵管理
　⑬アイデンティティ・アクセス管理
　⑭ストレージ
　⑮仮想化

全体で 83 ページの文書である．2008 年 12 月の発足から 5 カ月程度で，このように体系だったガイダンスの発行に至ったというのは，それだけ CSA の力が大きいことと，参加メンバが充実していたことを物語っている．

(B) クラウドコントロールマトリクス

クラウドコントロールマトリクスは，2010 年 4 月に発表された．CSA の Web ページに記載された紹介文によると，その開発意図は，クラウドのセキュリティについて基本原則を提供し，クラウドベンダのガイドになるとともに，ユーザのリスク評価の役に立つことを狙っている．CSA の Web には次のような説明文がつけられている．

「コントロールマトリクスは，CSA が提供するガイダンスの 13 の領域☆5 に対応した，セキュリティのコンセプトと基本原則を詳しく理解するための管理策のフレームワークを提供している．その基礎となっているのは，世の中に受け入れられているセキュリティ標準，規制，管理枠組みで，具体的には HITRUST CSF，ISO27001-27002，ISACA の COBIT，PCI DSS，NIST である．そしてクラウドプロバイダが提供する SAS70 証明書について内部コントロールの指示を与え，または強化する」

クラウドコントロールマトリクスは，excel ファイルの形で CSA の Web に掲載されており，誰でも自由にダウンロードして参照することができる．それはマトリクスの名の通り表形式で，縦軸にはコントロール（管理策）項目，番号，その内容説明が並んでいる．横軸は，SaaS・PaaS・IaaS のどれが適用対象か，プロバイダの遵守項目かユーザか，他の基準のどの項目に対応するか（コンプライアンス・マッピング）が示されている（図 -2）．コンプライアンス・マッピングで取り上げられている基準類は，COBIT，HIPAA，ISO/IEC27002-2005，NIST SP800-53，PCI DSS である．

縦軸の領域名を拾うと，コンプライアンス，データガバナンス，施設のセキュリティ，要員のセキュリティ，情報セキュリティ，法関係，運用管理，リスク管理，リリース管理，障害耐性（Resiliency），セキュリティアーキテクチャ，の 11 の領域区分があり，全体で 98 のコントロール（管理策）がリストされている．

クラウドの提供者または利用者がこの管理策項目の 1 つ 1 つについて合否を判定することで，各種基準に対する適合性も含めてセキュリティレベルの判断が可能になるように作られている．なお，98 の項目に対して，合格レベルの数字や点数によるレベル分けのような指標は特に示されていない．これは各コントロールの重み付け自体が一様でなく，また利用目的や利用環境によっても変化することを考慮して，一律のクラス分けを回避しているためと推察される．

(C) クラウドの重大脅威（Top Threats to Cloud Computing）

クラウドの重大脅威は，2010 年 3 月に最初のレポートが発表された．ユーザがクラウドを採用する際のリスク管理を支援することを目的としており，

☆5 Version 2.1 で 15 領域から 13 領域に整理統合された．

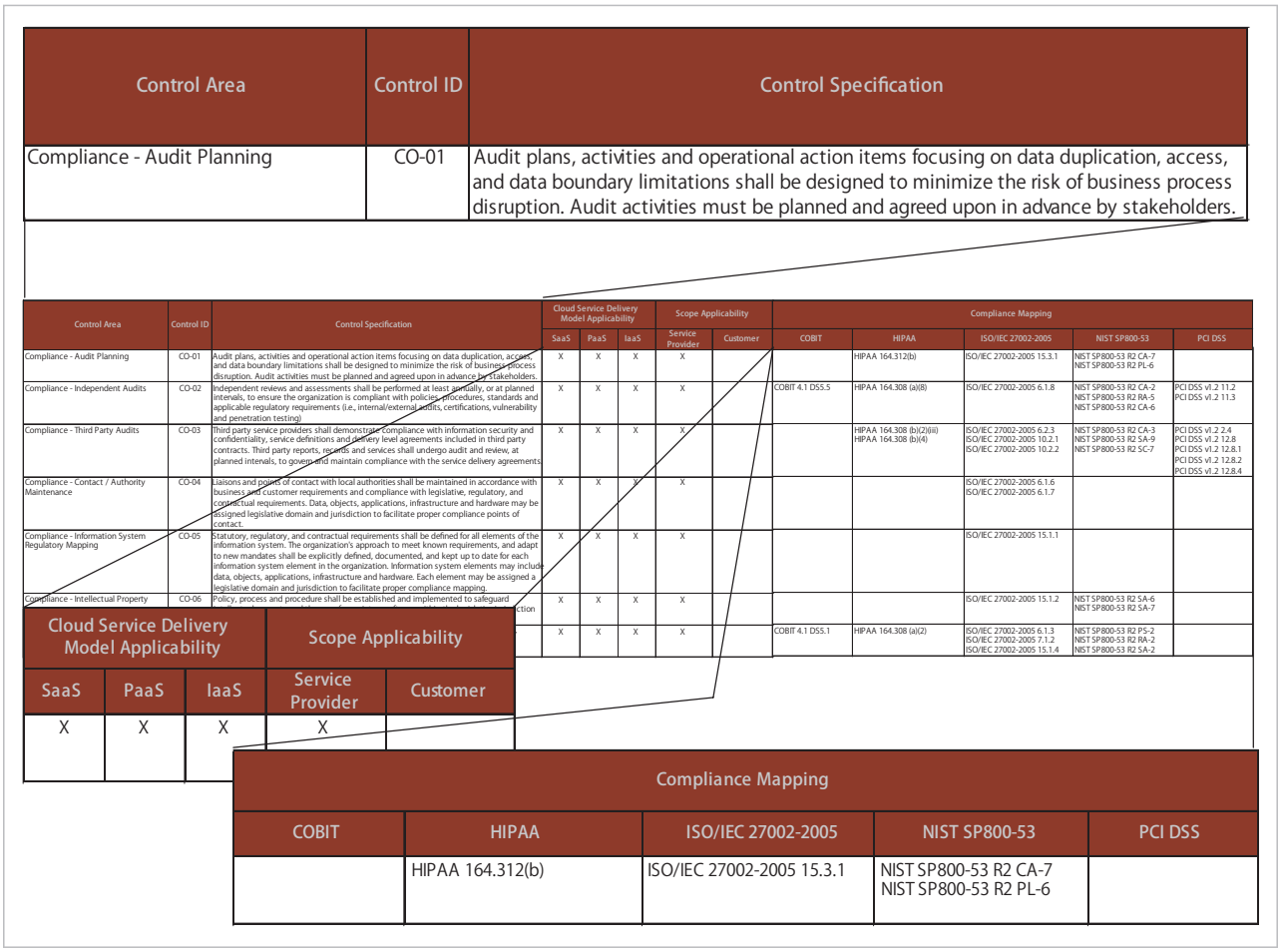

図 -2　クラウドコントロールマトリクスの表構成イメージ

クラウドセキュリティガイダンスの補助資料と位置づけられる．本レポートは定期的な発行が計画されており，クラウドセキュリティガイダンスに対するアップデート的役割を意図しているものと見られる．初版では，以下の 7 つの脅威が取り上げられている．

1) クラウドコンピューティングの悪用・不正利用
2) 安全でないソフトウェアインタフェースと API
3) 内部従事者の非行
4) 共有環境の技術問題
5) データの漏えいと紛失
6) アカウントまたはサービスの乗っ取り
7) 未知のリスク構造

(D) その他の研究テーマ

このほか，CSA の Web ページでリサーチのページを開くと，いくつかの研究プロジェクトが紹介されている．簡単に紹介すると：

1) Consensus Assessment Initiative：クラウドプロバイダのセキュリティ評価を一貫して提供するためのツールと手順を提供するもの
2) Cloud Metrics：セキュリティ対策の評価指標．クラウドプロバイダ側ユーザ側両用．Consensus Assessment Initiative のツールの一部としての利用も想定されている．
3) Trusted Cloud Initiative：クラウド上の安全で互換性のあるアイデンティティ管理

(以下パートナープロジェクト)

4) Cloud Audit：クラウドの監査に向けて，監査，アサーション，評価，保証を自動化できるようにする共通インタフェースの開発．A6 グループで取り組み中．
5) Common Assurance Maturity Model (CAMM)：

情報セキュリティ保証の成熟度を客観的に評価するための共通尺度の開発．ENISA（欧州ネットワーク情報セキュリティ庁）主導の国際・業際プロジェクト．

クラウドセキュリティアライアンスの日本における活動の概要

(1) 支部の仕組みと日本クラウドセキュリティアライアンス発足の経緯

日本クラウドセキュリティアライアンス(以下「日本 CSA」）は，2010 年 6 月 7 日に，CSA の地域支部としては世界で 3 番目に設立された．これは CSA が 2010 年になって定めた支部設立基準にのっとって，日本の有志によって設立されたものである．CSA で支部設立の要件として，20 人以上の設立時会員，5 〜 15 名程度の Board Of Directors（幹事会），支部固有の取り組みテーマ，支部のロゴを用意するように求め，活動としては，幹事会の定期的開催，普及イベントの実施，年次総会の開催，年次報告書の作成等を求めている．

個人がベースとなる組織で，会費負担の規定もなく，その意味でボランティアベースの活動を前提として想定していると言える．個人の参加手続きは，LinkedIn で会員登録申請し，そのグループの管理者に参加承認を受けることだけである．2010 年 8 月 25 日現在，日本支部には 167 人が登録している．日本以外には，スペイン，ブラジル，ムンバイ，中国，イスラエルが設立済みで，エジプト，イタリア，シリコンバレー，バンガロール，チェンナイ等が準備中である．

日本支部設立についての議論のきっかけとしては，CSA の創立者で事務局長を務めている Jim Reavis が ISACA 東京支部の招きで 2009 年 12 月に来日したことに端を発している．Jim との会食に顔をそろえたメンバの中から，日本での活動の母体を求める意見が出され，また CSA 側でも支部設立指針が 2010 年に入ってすぐ出されるなど，機が熟した感じで話が進みだした．啐啄同時といったところか．

(2) 情報処理推進機構との相互協力協定の締結および IPA グローバルシンポジウムでの基調講演

Jim Reavis 事務局長の 2 度目の来日は，2010 年 6 月であった．第一の目的は，IPA 主催による「IPA グローバルシンポジウム 2010」の基調講演者としてである．IPA は「クラウドコンピューティング社会の基盤に関する研究会」を開催しその報告書を 2010 年 3 月に発表するなど，クラウドコンピューティングに関する調査研究を進めるとともに，普及に向けての条件整備に多方面から取り組んでいる．その活動の一環として，CSA との間で相互協力協定を締結し，相互にその活動に協力していくことで合意した．その具体化の第一歩が，Jim Reavis 事務局長による「IPA グローバルシンポジウム 2010」での基調講演となった．両者は 6 月 7 日に調印式を行い，その概要はプレス発表された．

(3) 日本クラウドセキュリティアライアンス発足記念シンポジウム

日本 CSA 発足記念シンポジウムは，6 月 8 日午後に開催された．会場はインターネットイニシアティブ(株)のご厚意により提供された同社のセミナルームが使われた．定員を大幅に超える 200 名以上の申し込みを受け，急遽椅子席の追加等で対応して，何とか全員に聴講いただくことができた(図 -3)．

プログラムは以下の通りである．

1. 日本クラウドセキュリティアライアンスの意義
   勝見　勉／(独)情報処理推進機構(IPA)
2. クラウドコンピューティングの課題と CSA への期待
   加藤雅彦／インターネットイニシアティブ(株)
3. クラウドコンピューティングと eID マネジメント
   下道高志／ISACA 東京支部
4. CSA ガイダンスについて
   佐々木豊／NPO ASP・SaaS インダストリ・コンソーシアム
5. CSA の 2010 年のイニシアチブについて

図-3　日本クラウドセキュリティアライアンス発足記念シンポジウム会場風景

笹原英司／ヘルスケアクラウド研究会

6. 日本クラウドセキュリティアライアンスの活動と課題

高橋郁夫／弁護士

7. クラウドセキュリティアライアンスの今後の活動について

Jim Reavis／クラウドセキュリティアライアンス

8. フリーディスカッション

日本CSAの設立準備に携わってきたメンバを中心に，CSAとその日本支部を紹介する，網羅性の高いプログラムを実現できた．

フリーディスカッションセッションでは，筆者が司会を担当し，Jim Reavisはじめ講演者が質問に答えるかたちで活発な討議が行われた．テーマとしては，クラウド上のユーザ認証問題，暗号問題等技術的なテーマのほかに，日本CSAにおいて，法人が活動に参加できる枠組みについても質問が寄せられた．またクラウドにおける「トラスト」の課題も議論された．

シンポジウムのプログラムと発表の様子は，日本CSAのWebサイトで公開している．

http://www.cloudsecurityalliance.jp/

(4) 日本クラウドセキュリティアライアンスの今後の活動

日本CSAは，支部の独自テーマとして，「クラウドセキュリティガイダンス」の，「日本における実装と適用のためのガイド」をまとめることとしている．CSAによるガイドは，その組織が世界ベースのものとして活動しているとは言え，発足の地であるアメリカの事情を色濃く身にまとっている．したがって，それをそのまま日本で適用しようとしてもそぐわない要素も出てくる．その辺りを中心に，解説や補足を提供することで利便性の向上を図りたいと考えている．

典型的な例としては，法律関係がある．高橋郁夫弁護士を中心に，「クラウドセキュリティガイダンス解説版・法律編」が執筆編纂され，RSAカンファレンスJapan 2010において発表された．その内容はさらに加筆改訂されて，この文章が発刊されるころには日本クラウドセキュリティアライアンスのWebページから公開されている予定である．このほか，コンプライアンスと統制についても同時発行を目指して開発が進められている．

日本CSAの発足の意義は，このようにCSAの活動成果を日本に根付かせられる形で紹介し，日本での活用を促す機能を発揮することにある．個人のボランティアベースという制約の中で，参加者の意気と意思によって日本に役立つ活動を実現することを目指している次第である．

また，CSA本部から要求されている支部の義務として，普及啓発活動がある．こちらの方は，CSA幹部の来日等の機会を捉えて実現することが期待される．

今後の展望と課題：クラウドコンピューティングのセキュアな利活用に向けて

日本CSAの活動は緒に就いたところで，その具体的成果を挙げていくのはこれからの課題である．個人のボランティアベースの参加が土台となった組織なので，どこまで計画性と説明責任を持ってアウトプットを出していけるかは，難しい問題を秘めている．

また，日本国内のクラウド事業者からは，ユーザ

が安心して使ってくれるためには，業界共通の尺度でサービスやセキュリティについて説明できる必要を感じており，そのための共通尺度の開発等への期待が強い．同様に，トラブル等が発生したときにそれをハンドリングできる中立機関の存在や，顧客が国境を越えて利用するような場合の国際間の調整，あるいは国際的な共通理解形成といった期待も語られている．国際的な連携の面では，CSA のネットワークは利用価値が高いと期待されるが，ビジネスにかかわる機能を担うには，日本 CSA の枠組みでの対応は限界がある．このために，法人ベースでの活動を形成する場をいかに作るかは，課題として残っている．

一方で，クラウドコンピューティングがもたらす「所有から利用へ」の変化は，コンピュータシステムを利用する立場に対しては，設備投資，開発投資，運用負荷，保守負担等をクラウド事業者側に転嫁し，サービスの利用料をコストベースで払えば済むという大幅な負担軽減のメリットを生み出す．これを活かして，従来さまざまな負担がネックとなって十分に活用できなかった IT の恩恵を，経営に取り込んでいくチャンスとすることが期待される．特に中小企業における期待効果は大きい．

情報セキュリティ対策の面でも，クラウドは一定の効果をもたらすと期待されている．クラウドには，クラウドセキュリティガイダンスが指摘するセキュリティ課題も多く存在する．しかし，セキュリティ対策についての知識や経験が十分でないユーザが必要な手当てを行わずにいる状態に比べれば，データセンタに専門のセキュリティ要員を配置することも可能なクラウドサービスのセキュリティレベルは一般に高いと言える．たとえばファイアウォールのログ解析にしても，ウイルス対策ソフトの定義ファイルの一斉更新にしても，ユーザが自社内で完璧にこなすためには高度なセキュリティ人材を確保しなければならず，それは特に中小企業にとっては容易でない．このような問題の解決も，クラウドには期待されるところである．

その意味でも，クラウドコンピューティングの利活用が促進され，一定のセキュリティレベルが普遍的に確保される状態に到達することが期待される．そのためには，IT に必ずしも強くない企業も，セキュリティ要件も理解した上でクラウドを使いこなせるための環境整備が必要となる．IPA は，そこに向けて情報提供を行うとともに，啓発活動や環境整備にも取り組んでいる．

日本 CSA としては，普及啓発の面を中心に，CSA の世界に広がるネットワークも背景に，各方面とのタイアップも視野に入れ，クラウドコンピューティングの安全で積極的な活用の促進に取り組んでいきたいと考えている．

なお，本稿における意見や観測にわたる部分は筆者の個人的見解であることをお断りする．

参考文献

1）http://www.cloudsecurityalliance.org/
2）http://www.cloudsecurityalliance.jp/
3）http://cloudaudit.org/
4）http://www.enisa.europa.eu/
5）http://www.isaca.gr.jp/homepage_j.htm

（平成 22 年 8 月 31 日受付）

勝見　勉 t-katsu@ipa.go.jp

1990 年代半ばより国内電機メーカ，シマンテック，リコーグループ企業等でセキュリティ製品・サービスの輸入・普及・販売に従事．2008 年より情報処理推進機構研究員として情報セキュリティ，クラウドコンピューティングの研究・普及活動に取り組み中．（株）情報経済研究所代表取締役，NPO 日本ネットワークセキュリティ協会理事・幹事．日本セキュリティマネジメント学会会員．