パネル討論

情報セキュリティの今後のあり方

パネリスト　高橋 正和（（株）Preferred Networks CISO）
福本 佳成（楽天（株））
内田 法道 （（株）ラック）
小川 博久（みずほ情報総研（株））
菊池 浩明（明治大学）
モデレータ　中尾 康二（横浜国立大学先端科学高等研究院）

2018年3月13日に行われた情報処理学会　第80回全国大会の「現場から見た情報セキュリティの現状と今後―デジタルプラクティスライブ―」におけるパネル討論の内容を記録したものです．

高橋正和氏（（株）Preferred Networks CISO, Security Architect）
基本ソフトの開発や品質管理等を経て，1999年にISS（現在はIBM）に入社．コンサルティングビジネスの立ち上げ，SOC構築支援，CIOとして社内ITシステムの構築運用などを実施．2006年に，日本マイクロソフト（株）のチーフセキュリティアドバイザに就任．工作機械メーカ，自動車メーカのセキュリティアドバイザとしても活動．2017年10月，Preferred Networks CISO，セキュリティアーキテクトに就任．日本ネットワークセキュリティ協会副会長，日本セキュリティ・マネジメント学会常任理事．

福本佳成氏（楽天（株） ITセキュリティガバナンス部 執行役員 部長）
インターネットセキュリティ専門会社でセキュリティプロダクトの研究開発を経て，2002年に楽天（株）に入社．楽天グループのインターネットサービスのセキュリティを担当．主には安全なソフトウェア開発の推進とセキュリティ運用を担当している．2007年にRakuten-CERTを設立．Rakuten-CERT Representative．活動開始時よりOWASP Japan Advisory Boardを務める．東京工業大学サイバーセキュリティ特別専門学修プログラム特定教授．近年はサイバー犯罪対策にも注力している．

内田法道氏（（株）ラック IT統括本部 サイバーセキュリティ事業部，サイバー救急センター センター長）

1999年（株）ラック入社．1999～2000年セキュリティ製品サポートに従事．2001～2005年セキュリティコンサルタントに従事．2005～2007年内閣官房情報セキュリティセンター（現：内閣サイバーセキュリティセンター）で勤務．2007～2013年セキュリティコンサルタントに従事．2014年ネットワークフォレンジック調査に従事．2015～現在サイバー救急センターのセンター長としてインシデント対応に従事．

小川博久氏（みずほ情報総研（株） 経営・ITコンサルティング部 マネジャー）

2000年にソフトウェアベンダに入社し，取締役R&D事業本部長を歴任．暗号モジュール設計・開発，情報セキュリティ，リスクマネジメント等に関する研究開発業務を統括．2008年，みずほ情報総研（株）に入社．情報セキュリティ技術に関する調査および研究開発業務に従事．日本ネットワークセキュリティ協会（JNSA）電子署名WGサブリーダ／リモート署名TFリーダ，日本トラストテクノロジー協議会（JT2A）運営委員長．

菊池浩明氏（明治大学 総合数理学部 教授）

1990年明治大学院博士前期課程修了．1994年同博士（工学）．（株）富士通研究所，東海大学情報通信学部を経て，2013年より明治大学総合数理学部先端メディアサイエンス学科教授．1990年日本知能情報ファジィ学会奨励賞，1993年本会奨励賞，1996年SCIS論文賞，2010年，2017年本会JIP Outstanding Paper Award．2013年 IEEE AINA Best Paper Award．電子情報通信学会，日本知能情報ファジィ学会，IEEE，ACM各会員．本会フェロー．

中尾康二氏（横浜国立大学先端科学高等研究院）
1979年早稲田大学卒業後，国際電信電話（株）に入社．KDD研究所を経て，現在KDDI（株）顧問，および国立研究開発法人情報通信研究機構（NICT）サイバーセキュリティ研究所　主管研究員，横浜国立大学　客員教授を兼務．ネットワークおよびシステムを中心とした情報セキュリティ技術／サイバーセキュリティ技術の研究開発に従事．電子情報通信学会，本会などの会員．経済産業省大臣表彰賞，KPMG情報セキュリティアウォーズ，文部科学省大臣表彰賞，情報セキュリティ文化賞，総務大臣表彰等を受賞．2017年から内閣官房　サイバーセキュリティ補佐官を担務．

中尾　講演が盛り上がったおかげで残り時間が30分ほどになってしまいましたが（笑），ここからは「情報セキュリティの今後のあり方」についてみなさんとディスカッションしていきたいと思います．具体的にどんな課題があるのか，そのために我々は何をやっていくべきなのかについて，現場のベストプラクティスの話から，よりアカデミックに考えるとしたらどういうことができるのか，といったことまで幅広く議論できればと思います．まず5名のパネリストの方にお一人ずつ気になっていることをお話しいただいて，それから会場の方からもコメントやご質問を伺い，それらをまとめていくという進め方でいきたいと思います．では，まず福本さんからですが，みなさん，適度な長さでお願いします（笑）．

福本　また長くなるかもしれませんが（笑），私の講演では「SOC☆1構築とセキュリティ監視運用の取り組み」というお題で，私が所属する楽天が展開するインターネットサービスのセキュリティ対策全体におけるSOCの役割や変遷，留意事項について紹介させていただきました（「SOC構築とセキュリティ監視運用の取り組み」参照）．

今後のことについていえば，SOCというものはもうやって当たり前のこととなってきていて，今からSOCを頑張りましょうというのではなく，これから先はよりプロアクティブなセキュリティを考えるべきだろうと思っています．

最近でもWannaCry☆2で大騒ぎになったところがありましたが，あれもきちんとパッチを当てていたら全然何でもなかったわけですよね．でも，そういった大騒ぎはとても多い．そういった大騒ぎをしなくてすむような，そもそも安全なものづくりやシステム環境づくりができないかなと．

最近，CSIRT☆3が注目を浴びていて，その活動はもちろん大事なのですが，それがあるせいか最近は「やられないシステム」を作ることを諦めかけている風潮があるような気がしていて．マルウェアは防ぎ切れないものだ，とか言うのではなく，今こそ基本に立ち返って，守り切る方法のようなことに注力していきたいと思います．

そのためにはCISO（Chief Information Security Officer）が大事だろうと思っています．プロセスを根本から変えるというのは心底パワーがいることなので，技術もセキュリティも人も分かる，全部分かっているCISOという存在がキーになるのではないのかと思っています．

高橋　私の講演では，「業務執行としてのセキュリティ」というお題で，経営に役立つセキュリティ業務やその報告内容とはどうあるべきかをお話させていただきました．実際にCISOあるいはセキュリティ担当として現場に入って感じたのは，セキュリティのちょっとした判断は日常

茶飯事で，経理の専門家や法律の専門家が必要なのと同じくらい企業にはセキュリティの専門家が必要だ，ということです．というのも，広範なセキュリティを分類してそれぞれを別々に考えるのは難しいからです．たとえば，情報セキュリティのリスクというのはどう扱うべきか，あるいは，IDカードや入退出管理などのフィジカルセキュリティはどうなっているのか，といった個別の話題で大激論になったりします．しかし，それらはコーポレートリスク全体の中の一部であって，完全に分けて考えることはできません．たとえば，エンタープライズ・リスク・マネジメントという相当完成された手法があります．完成しすぎていてちょっと手が出しにくいところがありますが（笑）．ただ，そういったものを出発点として，広範囲な話題を議論する基盤のようなものを発達させる必要があるのだと思います．

先ほど福本さんと話していたのは，最近の，特に日本では，あまり経験のない人たちがCISOに就くことがしばしばあるということです．そんな状況の中で日本のセキュリティを保っていくことはますます難しくなってくるだろうと思っています．

内田　私は「高度標的型攻撃におけるインシデント対応の理論と実践」という論文を寄稿させていただきました（「高度標的型攻撃(APT)におけるインシデント対応の理論と実践」参照）．

標的型攻撃を行う攻撃者は，一度攻撃をしてから半年後くらい，対処が完了したくらいのころにもう1回標的型メールを送ってきたりします．そういった，攻撃者が用いるマルウェアやサーバ，インフラに関する情報がいわゆるインテリジェンスとして共有され，攻撃対策に利用されていますが，攻撃者側もそれらを進化させるために両者の間でいたちごっこが続いています．いたちごっこを繰り返さずにすむように，私たちのほうが一歩先を読めるような形でインテリジェンスを活用できないかということを最近考えています．

余談になりますが，昨年（2017年）末くらいからあちこちの大学や研究機関が狙われているように思います．この会場には大学の方も多くいらっしゃるようですので，気を付けていただけたらと思います．

中尾　余談とおっしゃいましたが，私も標的型攻撃の研究をしているので，質問させてください．大学や研究機関が狙われているとのことでしたが，それは大学系や研究機関系を広く狙ったばらまき攻撃のようなものですよね．それとも，いわゆる標的型攻撃なのでしょうか．

内田　後者，つまり，特定の大学や研究機関を狙った標的型攻撃のことです．

中尾　それは対策するにも厄介ですね．

高橋　横から口を挟んじゃいますが，大学のセキュリティの先生というのは，大体，セキュリティ対策をしていないですよね（笑）．

菊池　そんなことはないと思いますよ（笑）．

内田　逆に進んでいるところもあるのですが，やはり元々セキュリティと相性が悪い文化があるのではないかと思いますので，お気をつけいただければと（笑）．

中尾　ではそのくらいにして（笑），次は小川さん，お願いします．

小川　私は電子署名について講演させていただきました（「デジタル社会のトラストを支える電子署名」参照）．それに関する課題というと，セキュリティ技術者がシステムを設計したり構築したりするとかなり堅めにしすぎて使い物にならなくなるということがよくあるように思いま

す．たとえば，ハードウェアのトークンの鍵をなぜ出せないのか？とか，いったん，事業者に預けた鍵がなぜ出せないのか？と怒られてしまうとか，一般の人の理解や必要とするものとのギャップが大きくなりがちなように思います．

ベストプラクティスということでいいますと，電子署名の利用促進をどうするかがあると思います．欧州はそのための制度をつくったりして，その地域の力にしています．一方，アメリカではもう実際にビジネスで普通に使われているような状況です．日本はどうなのかというと，電子署名の利用環境を整えるためのパーツがコントロールできないのですよね．ブラウザもOSも日本勢は抑えていないですし．ただし，電子署名を利用するサービスは出てきているという状況です．なので，どちらかというと欧州に似ているのですが，サービスの面ではアメリカに近いところもあります．ベストプラクティスということとは逸れてきましたが，欧州ともアメリカとも話が通じるのは良いところと思っています．

中尾　リモートで電子署名をするという技術や事業について，日本ではどれくらいの潜在的な需要があると見込まれているのですか．

小川　需要はあると見込んでいます．JT2A☆4という協議会が立ち上がったのもそのためですし，電子契約元年といわれたのが確か3年くらい前ですが，メーカも製品も増えてきています．具体的な利用例としては，長期融資であるとか，あるいは，建築関係，医療関係などでもすでに使われています．

中尾　なるほど，ありがとうございました．では，菊池さん，お願いします．

菊池　今日の講演者やパネリストの皆さん，特に，福本さんと平山さんの話（それぞれ，「SOC構築とセキュリティ監視運用の取り組み」，「2020年を超えて生き抜くセキュリティ人材の育成と多様性への対応 ―必要とされるセキュリティ人材の変化と 育成方法の視点より―」参照）を聞いていて思ったのは，やはりセキュリティ人材が足りないという課題です．たとえば，セキュアコーディングやフォレンジクスとか，実装周りが分かる技術者の不足はまさに痛感しています．その一方で，私は大学の教員でもありますので，教えることの難しさも実によく痛感しています．

昨日，先のセメスターの授業評価アンケート結果が来ましたが，平均よりはるかに下回っていました（笑）．大体，教員が気合いを入れて一生懸命話すのに限って評判が悪いのですね（笑）．手を抜いていい加減にしゃべると，割と評判が良かったりします（笑）．

それはさておき，私が大学で授業をするとしても，暗号はサンプルや短いコードでアルゴリズムを示して教えられるのでやさしいのですよ．しかし，セキュアコーディングとかフォレンジクスというのは，システムのかなり細かいところまで話さないと面白味が伝えられないし，仮に教えたとしても，実際に社会に出て使うシステムはそれと同じとは限らないので，とても教えにくいと思っています．

ですから，そういった人材の育成の重要性についてはとても同感するのですが，それを教えようとするとまた評価が下がるなあ，というわけで（笑），以上です．

中尾　パネリストの皆さんからそれぞれお話をいただきましたが，会場の皆さんの中に，これを議論してほしいとか，ご意見，ご指摘，ご提案がございますでしょうか．

平井　先ほど講演させていただいた平井です．私はCSIRTとアナリストの中間みたいなところでリサーチをやっていて，情報共有も含めたCSIRTの役割について話をさせていただきました（「企業におけるCSIRTの活動とそれを支援する情報共有システム」参照）．情報源については，たとえばアメリカでいうとAIS（Automated Indicator Sharing）だったり，イギリスでいうとCiSP（Cyber Security Information Sharing Partnership）だったり，いろんな情報を集約してくれるところが増えてきました．日本国内でもセキュリティベンダがたくさんの情報を提供してくれます．けれども，情報が増えすぎてしまって，結局のところ全部は見きれない．だから適切な対処をやりきれないという事態が起きてしまうのではないかと感じています．WannaCryについても，パッチが3カ月前に出ていたといいますが，それが出た時点で必要性を正しく認識できたかというと，できなかったからああいう事態になってしまったわけです．

こういった，洪水のように溢れて流れている脅威情報の中から必要な情報をどうやって抽出すべきか，重要視すべきかといったことについて，何か知見のようなものをお持ちでしたら，ぜひ伺いたいと思います．

中尾　ご意見がある方はいらっしゃいますか．

高橋　若干，前職のにおいが残りますけれども（笑），1つは，SaaS（Software as a Service）を使うことでそういった情報の洪水から解放される，ということがあると思います．メールサービスなどは自前でやらずとも手放せばよいだろう，ということです．では，SaaSベンダがなぜ脆弱性対応を適切にできているかというと，たとえば，仮想化を使って問題があったら切り戻すというようなやり方をしている．もし自前でやるのであれば，SaaSベンダと同じような仕組みと手順にしていく方法があると思います．

それから，先ほどの平井さんの問いかけの中には，情報の重要度をどうやって切り分けるのかということと，それからどうやってパッチを当てて運用するのかということの2つの論点があると思います．前者の情報の重要度なんていうのは，もう分からないのだと思います．WannaCryのケースでいえば，明らかにやばいというのは分かる人は分かる．でも，そうじゃないのにもやられるときはやられる．そう考えると，出てきたものを当てざるを得ない．ですので，繰り返しになりますが，自分でパッチを当てなくてすむ環境に変える，もしくは，しっかり運用できているところと同じ運用をするように変えて行く，ということが解決策になるかなと思っています．

中尾　私はICT-ISACにかかわっていまして，平井さんのおっしゃったAISも含めていろんな情報を集めて共有しています．AISというのはアメリカのDHS（米国国土安全保障省）が進めている情報共有スキームですが，アメリカで集めた情報があれこれと洪水のようにやってくる．それらをどうやって活用するのか，という課題意識はICT-ISACにもあります．

それについては，たとえば，IPアドレスとマルウェアとの関係性だとか，マルウェアとC2サーバ☆5の関係性といったところに着目してコリレーション（相関関係）を抽出し，結果を使うようにすれば，見るべき情報はぐっと少なくなって使いやすくなるのではないかと思っています．

C2サーバはどんどん変わりますし，マルウェアもどんどん変わる．ブラックIP（悪性IPアドレス）がどういう使われ方をするかも変遷がある．そういったことも含めて，コリレーションをうまく取れるようなデータ加工というのが今後のコアになる気がしています．

中尾　それでは残った時間で，いろいろな意見が出てきたCISOについて少し議論していきたいと思います．言い足りなくてうずうずしている人が何人かいらっしゃいますし（笑）．

CISOは皆さんご存知だと思います，Chief Information Security Officerの略で，企業において情報セキュリティに関する責任を持ち，経営判断に近いことも含めて実施する役職です．私の知る限りでは，技術統括本部長などといった高位の役職を持つ人がアサインされることがほとんどです．偉い人がやっているので，当然，セキュリティの専門家ではないことも多いのです．そうすると，福本さんみたいな方が裏で一生懸命やる必要があるわけです．

欧米のCISOはセキュリティのことを本当によく知っています．CISOの位置づけが，日本と欧米とでは全然違うのです．しかし，そこは変えていかなくてはいけない，またはその構造上の問題点をちゃんと認識しなくてはいけないと思います．このことについて，ご意見いただければと思います．

福本　若手の育成と同様にCISO人材の育成もやはり大事だと思っています．楽天グループではCISOを39人立てましたが，CIO兼CISOの方が半分ぐらいです．残りの半分はリスク・ガバナンス系の人で技術はあまり分からないという人も結構います．海外を見るとCISOトレーニングなども結構あるので，そういったものを受けさせるなり，何か手を打たなければいけないと思っているところです．

もう1つ問題だと思っているのは，CISOに任命された人はみんな嬉しそうじゃないことですね（笑）．基本的に良い報告をすることは少ないし，インシデント発生時には社を代表して謝罪をすることもあるし，あまり良いことがない．その割に学ばなければいけないことも多く，高いレベルで要求されるし，責任もある．CISOになりたいという人が世の中にどれだけいるのかな，と思ってしまう．やはりCISOになるインセンティブだとか，CISOはかっこいいみたいな憧れだとか，そういったものが増えていかないと，CISOのなり手はなかなか増えないのではないかと思います．高橋さんにはそういったロールモデル，憧れのCISOになっていただきたいと思います．ということで，高橋さんにパスします（笑）．

中尾　高橋さんは，今，CISOなんですか？

高橋　CISOのポジションで入社したわけではないのですが，入社した翌日に「はい」と渡されまして，それからCISOをやっています（笑）．

あえて少しずらした話をすると，今いる会社のITシステムはほぼクラウドなのです．IT部門の人間が本当に少人数で，その一方で自前でスパコンを作ったりしている会社なんですね．そういう環境なので，CISOでやっていくのが楽な部分とそうではない部分があります．楽な部分というのは，ITシステム全体が比較的見えやすいところです．一方，楽じゃない部分は，研究所がそのままベンチャーになったような会社なので，一般の企業のような統制が難しい面です．そこで今少し苦労しているところがあります．前者の話をすると，このくらいの規模であれば担当者とじっくり話をして，お互いの考えをすり合わせて，その方向に持って行くということがやりやすいと思います．オンプレミスでガリガリ作っているようなところのCISOとはかなり違うのだろうと思っていて，今後，クラウドベースのITのセキュリティについて，まとめていきたいと思っているところです．

内田　私もインシデント対応の中でCISO対応をすることがあるのですが，CISOはちゃんと決断をして責任を取ってくれさえすれば，それでよいと思っています．技術的なところは福本さんのような有能なアドバイザがいればすみますから．CISOはそういう権限と責任をセットで引き受ける覚悟のある人であればそれでよいと思います．では，有能なアドバイザをどう育てるか，というのが難しいところですが．

小川　高橋さんがいるのであまり言いたくないのですが，日本のCISOで，「ああ，この人，なるほど」という人があまりいない（笑）．だから，もしかすると私は日本にはCISOというのは本当はいない，あるいは，いらないのではないかと思っています．イエスかノーかを判断してくれる箱があれば，たとえ，判断が間違えていようがいまいがそれで会社は回るのではないかと思っています．だからどうだということはないんですが．

高橋　案外そうかもしれないですね（笑）．ただ，日本では，CISOだけではなく，オフィサー制度がそもそも馴染んでいないのですよ．CISOにだけ注目すると小川さんのような印象を持たれるかもしれないですが．ただ，日本の中でもベンチャーや若い企業を中心にオフィサー制度で上手くいっているところも出てきていますので，その辺りも変わってくるだろうと思っています．

中尾　では次の話題に行きましょう．攻撃手法やマルウェアを作るスキルが向上してきている中で，我々守る側や研究する側として何をやるべきかということが，人材育成と合わせて重要になってくるでしょう．たとえば，何かの挙動から予兆を把握したり，近い将来起こることを予測してプロアクティブに準備したり，あるいは，そのための観測網を日本の中で作ったり，ということが必要になると思います．ひょっとしたら認証やプライバシーに関する課題でも出てくるかもしれません．その辺りについて，本当にひと言ずつ手短かに（笑）いただけますか．

菊池　うまい情報シェアリングのスキームというのは欲しいですね．NICTさんにはすごい観測データベースがあると伺っています．そういった生データをコントラクトを交わしてちゃんと共有できる仕組みを作っていかなければいけないということは常々感じています．

内田　私のところではインシデント対応の際の機密保持契約を見直していて，お客さまの情報を匿名化して必要な外部機関に共有できるようにしてあります．たとえば，法執行機関やセキュリティ関連機関などに，インシデント情報で関係するものは共有していこうという取り組みをしているところです．もちろん，逆に提供していただけるようになることも含めて，そういった横の連携がもっと進められるとよいと思っています．

高橋　また別の視点からの話になるのですが，今やマイクロソフトやグーグル，アマゾンといったいわゆるハイパージャイアントのところに，あらゆるネットワーク情報が集まっていて，それをすべてアンチウィルス等にかけてゼロデイ系☆6の検知もやって，というのが現状です．こういうハイパージャイアントたちとどういう風にやっていくのか，という視点が必要だと思っています．正面から挑んでいって勝てるとは考えにくいのですが，かといって日本は何もしなくていいのかというと，私はそうは思わない．ハイパージャイアントたちとどううまく付き合うか，もしくは，日本独自の強みをどうやって作っていくか，そういう視点を常に持っていなければならないと思っています．

福本　自分の講演が終わったあたりまさにアタックが始まって，先ほどまで携帯電話で対応をしていたところです（笑）．攻撃ということでは，ボット☆7を使った不正ログインはまだまだ結構厄介です．マシンラーニングを使ってボットを検知して，見つけたらロックするというような仕掛けにはしてあるのですが，向こうも少しずつ改良してくるので，どうしてもいたちごっこになる．突破されてブロックして，突破されてブロックしてというのを繰り返しています．昔からいたちごっこではあるのですが，昔はこんな量ではなかったのですよ．今や弊社に来るトラフィックの30％がボットからのものになっている．そういう状況を打破するのが1つのテーマと思っています．

そもそもIDとパスワードの認証は，だれもパスワードを覚えられないし，無理があると思っています．たとえば，攻撃を受けてアカウントをロックをしてパスワードをリセットしたあとに，わざわざ不正ログインされたパスワードに戻すユーザさんもいるのですよ（笑）．これでは対策にならないし，FIDO☆8はまだまだスタンダードとはいえないし，どうするのだろうなと．そうはいっても，何かのテクノロジーで乗り越えないと，このアタックは運用で対処していくのはかなりきついと思っています．

中尾　さて，ここまでセキュリティの視点でいくつか話題がありましたが，最後にプライバシーの視点に関して菊池さんに伺いたいと思います．私は現在IoTのセキュリティに関する研究もしているのですが，IoTも含めてセキュリティだけではなくプライバシーをどう考えていくかが重要だと思います．匿名化技術などプライバシーに関する技術をどういう風に世の中に入れていくのか，お考えはあるでしょうか．

菊池　個人的にはいくつか野望はあるのですけれども（笑），理想としては，従来のセキュリティ技術と同じように，オープンでパブリックなリソースにしていくことだと思います．たとえば，暗号でいうとAESやRSAなどがそうでしょうし，電子透かしなど，既存の技術にはどんどんオープンソースになって広く使われるようになったものがいくつもあるのです．匿名加工などのプライバシー保護技術もそういう形でどんどんパブリックになっていって共有されていくというのは1つのモデルだろうと個人的には考えています．

中尾　ありがとうございました．それでは，パネリスト，そして，オーディエンスの皆さん，どうもありがとうございました．

左から：福本佳成氏，高橋正和氏，内田法道氏，小川博久氏，菊池浩明氏

脚注

☆1　Security Operation Center．企業等に設置されるセキュリティ専門組織であり，ネットワーク装置やセキュリティ機器などの常時監視を通じてサイバーセキュリティ・インシデントの発見や特定，関連組織への連絡などの役割を担う．

☆2　ランサム型のマルウェアの一種．2017年に日本を含む世界中で猛威を振るった．

☆3　Computer Security Incident Response Team，企業等に設置されるセキュリティ専門組織であり，サイバーセキュリティ・インシデントの発生時には，その原因や被害状況の調査，対応策の検討，関連組織との調整などの役割を担う．平時にはインシデントの予兆を把握するモニタリング調査等を行う．

☆4　Japan Trust Technology Association．日本トラストテクノロジー協議会．

☆5　C2サーバ：Command&Controlサーバの略．C&Cサーバともいう．ボットに対して攻撃に関する指示を出し，その動作を制御する司令塔の役割を持つ．

☆6　ゼロデイ（攻撃）：まだ知られていない，あるいは，知られてはいるが修正パッチ

等の対策手段がない状態の脆弱性（を悪用した攻撃）．
☆7　元々は決められたタスクを自動的に実行するプロセスやプログラムを意味するが，ここではパソコン等に感染し，C2サーバからの指令に基づいて情報漏えいやDoSなどのサイバー攻撃を引き起こすマルウェアのことを指す．多数のボットがC2サーバにより組織化され，DDoS等の大規模なサイバー攻撃を引き起こすことも多い．それら全体をボットネットとも呼ぶ．
☆8　2012年に発足したFIDO Alliance（Fast IDentity Online Alliance）で標準化が進められている生体認証技術や多要素認証技術を活用したオンラインユーザの認証方式．多数のパスワードを管理する負担や弊害の解消を志向している．