**終わる「セキュリティ至上主義」、拡がる「セキュリティ格差社会」**

[**https://www.sbbit.jp/article/cont1/35611**](https://www.sbbit.jp/article/cont1/35611)

**徳丸浩氏×三輪信雄氏×石川滋人氏 対談**

ランサムウェアやビジネスメール詐欺（BEC：Business Email Compromise）など、サイバー攻撃は手を替え品を替え、企業に襲い来る。一方で、クラウドの広がりやテレワークの推進など、企業を取り巻く技術的・社会的な環境も変化している。こうした中で、企業はどのようにセキュリティを考えるべきか。キヤノンマーケティングジャパン セキュリティソリューション企画部 部長 石川 滋人氏がファシリテータとなり、Webセキュリティの専門家であるEGセキュアソリューションズ 代表取締役 徳丸 浩氏、総務省の最高情報セキュリティアドバイザー（CISA）を務めるS&J 代表取締役社長 三輪 信雄氏のお二人に、企業を取り巻くセキュリティの現状と課題について語ってもらった。

左から三輪 信雄氏、石川 滋人氏、徳丸 浩氏

**「セキュリティ至上主義」の考え方は改める時期にきている**

**石川氏：**まずは、現在の企業・組織が置かれているセキュリティ状況について、専門家としてのご意見を伺えますか。  
  
**三輪氏：**もう20数年、セキュリティに関わっていますが、本質的なところは何も変わっていないと思います。コンピュータウイルスは昔から存在しますし、サイトへの攻撃も90年代からありました。攻撃の手段も大きく変わっていませんので、守り方も本質的には変わっていません。にもかかわらず、メディア等で事件が報道されるたびに大騒ぎになるのは、本質が分かっていないからだと思います。  
  
**徳丸氏：**私も本質は変わっていないと思います。目的も、大きくは変わっていませんが、質的な変化はあります。具体的には、マネタイズの手段として新しいものが出てきました。たとえば、仮想通貨のマイニングをWebサーバや閲覧している人のPCでやるといったことです。ただ、これも改ざんの一種なので、対策は変わっていないのです。  
  
**石川氏：**一方で、企業はクラウドを積極的に活用するようになりました。こうした企業側の変化とセキュリティの関係はどう見ていますか。  
  
**三輪氏：**クラウドを使うようになると、もはや一律のセキュリティは成立しません。全員シンクライアント、PC持ち出し禁止、USB禁止、業務に無関係のサイトは閲覧禁止……。こういったすべてを縛るセキュリティでは、企業として成長することは困難です。その意味では、「セキュリティ至上主義」の考え方は、改める時期にきていると思います。  
  
　ちなみに、平成29年5月に閣議決定された「世界最先端IT国家創造宣言・官民データ活用推進計画」では、「クラウド・バイ・デフォルト原則の導入」という方針が打ち出されました。これは、政府関連のシステムを構築する際には、パブリッククラウドを最優先に検討するという方針です。

S&J 代表取締役社長  
三輪 信雄氏

**石川氏：**政府がパブリッククラウドを認めたということですね。  
  
**三輪氏：**はい。すると「クラウドはいいものだ。安心だ」となりがちですが、決してそうではありません。クラウドにはクラウドのセキュリティ対策がありますから、そこを理解しないままクラウドに飛びつくのは危険です。  
  
　これからはセキュリティを外部ベンダーに丸投げするのではなく、アクセス制御を含めて自分達で考えて、本当に必要なセキュリティを自ら構築する必要があると思います。

**クラウドによって変わるセキュリティの考え方**

**三輪氏：**最近のセキュリティ関連で気になっているのは常時SSLです。データが暗号化されるので、ネットワークの入口と出口にプロキシやファイアウォールを置いて監視する従来の手法が使えなくなります。通信の中身を見て、危険なURLやマルウェアを含むコンテンツをフィルタリングできなくなるので、従来のゲートウェイ監視の在り方は、変えざるを得ないと感じています。  
  
**徳丸氏：**日本の情報システム部門は、ネットワークの境界で守りたがります。それはそれで、いいことがたくさんあります。たとえば、世界で猛威を振るったランサムウェア「WannaCry」ですが、日本での被害は比較的少なかった。これは、境界での守りが強固だったからです。  
  
　ただし、いつまでも境界防御でいいのかというと、まったくそんなことはありません。クラウドになれば、会社の外に情報資産が出て行くわけですから、考え方を大きく変える必要があります。  
  
　常時SSLも、そういう文脈でとらえると分かりやすいでしょう。会社の資産が外にあるので、SSLが必須になるのです。これで盗聴は防げますが、認証とアクセス制御はより重要になってきます。やはり、従来の境界型の考え方を変えて、クラウドに適したセキュリティを勉強し、慣れなければなりません。

EGセキュアソリューションズ 代表取締役  
徳丸 浩氏

**石川氏：**エンタープライズの領域では、Office 365が大きな転換点、もしくはトリガーになると考えています。2020年1月にはWindows 7、10月にはOffice 2010のサポートが終了します。Windows 10とOffice 365への移行が一気に進み、クラウド化も進むでしょう。  
  
**三輪氏：**Office 365にすれば、スパムメールやメールのウイルスチェックも行ってくれます。ただし、2要素認証はしっかりやらなければなりません。こうした「クラウドに任せること」と、「こちら側でしっかり対応すべきこと」を区別して、バランスをとることが重要になります。

**脆弱性がなくならない原因は、開発の「格差社会」にある**

**三輪氏：**徳丸さんと対談できるということで、ぜひお聞きしたいと思っていたのが「脆弱性」についてです。私は前職で脆弱性診断をやっていたのですが、そのとき「この仕事はいずれなくなる」と思いました。しっかりした作り方をすれば、脆弱性は発生しないからです。それが15年ほど前の話ですが、いまだになくなっていません。こうした状況は、これからも続くのでしょうか。  
  
**徳丸氏：**確かに、いいツールを使ってセキュアな作り方をすれば、脆弱性はほぼ発生しません。ただ、これは2008年あたりからなのですが、開発における“格差社会”が広がっていると考えています。  
  
　しっかりとした教育を受けて、セキュアプログラミングに習熟し、「SQLインジェクションなどありえない」という開発者がいる一方で、クラウドソーシングによく見られるような、信じられない低コストでECサイトの構築を請け負う開発者もいます。こういう人たちがセキュアプログラミングできるかというと、厳しいのが実態です。  
  
　しかも、クラウドソーシングに丸投げするような案件では、そもそも脆弱性診断をしていません。従って、「脆弱性診断ではSQLインジェクションが減っている」といった統計が出るにもかかわらず、現実には脆弱なサイトがたくさん存在することになります。  
  
**三輪氏：**なるほど、格差社会ですか……。開発者全体が増えて、セキュアプログラミングができる層とできない層に分かれているということですね。だとすると、セキュアプログラミングを身につけたかどうかを証明する資格があるとよいかもしれませんね。  
  
**石川氏：**発注する側としては、信頼できる人や会社に頼めると安心ですね。

キヤノンマーケティングジャパン  
セキュリティソリューション企画部 部長  
石川 滋人氏

**徳丸氏：**最終的には国家資格みたいな仕組みがあればよいのでしょうが、現段階では敷居が高いのが現実です。ただ、ECサイトのような顧客のお金を扱うサイトを構築するのであれば、最低限の力量は保証されるべきだと考えます。

**「なあなあ」になりつつある現在の脆弱性診断**

**三輪氏：**もう1つ聞きたかったのが、最近は脆弱性診断が「当たり前」になっていないか、ということです。以前は、脆弱性の報告会は緊迫感がありました。開発ベンダーにとっては、自らのミスを第三者に指摘されるわけですから。ところが最近は……。  
  
**徳丸氏：**脆弱性を発見すると、むしろ開発ベンダーに感謝される。  
  
**三輪氏：**そうです。そして「修正しました」で終わってしまう。脆弱性診断が開発プロセスの中に当たり前のように組み込まれて、緊迫感がなくなってしまった。本来、脆弱性が発見されたら、開発プロセスを見直さなければならないのに、それがないがしろにされているように思えます。  
  
**徳丸氏：**おっしゃる通りです。脆弱性が見つかったら、開発ベンダーはプロセスを改善しなければならないし、その数が多ければ、発注側はベンダーの変更も含めて検討すべきなのです。ところが、発注側も“勝手知ったる”開発ベンダーなので変えたくない。  
  
　それに関しては、面白いエピソードがあります。ある会社で脆弱性診断の報告会を実施しました。経営者（サイトオーナー）、開発ベンダー、診断を行った私が参加し、発見された脆弱性を淡々と報告していきました。  
  
　すると、経営者が突然、「徳丸さん、話を聞いていると悪いことばかりおっしゃいますが、何かよいことはないんですか？」と言い始めたのです。よいことを褒める場ではなく、“脆弱性”診断の報告会なのに、なぜかベンダーの肩を持つんですね。誘拐事件で被害者が犯人に対して好意的な感情を抱く「ストックホルム症候群」という現象がありますが、それと似ているかもしれません（笑）。  
  
**三輪氏：**緊張感のない「なあなあ」の関係同士でやっているから「見つけました」「直しました」になってしまう。深刻な脆弱性が見つかったら、何らかのペナルティを課す仕組みが必要かもしれませんね。

**最新の攻撃手法や、クラウド・テレワークによって変わるセキュリティの考え方を解説**



**石川氏：**徳丸さんは、6月に著書『体系的に学ぶ 安全なWebアプリケーションの作り方』を改訂されました。かなりページ数が増えたようですが、その内容について簡単に教えていただけますか。  
  
**徳丸氏：**本質は変わっていません。ただ、Webを作るテクノロジーが多様化したので、それに合わせて内容を改訂しました。簡単にいうと、以前はサーバ側で処理していたのが、現在はクライアント側のJavaScriptでさまざまな処理をするようになった結果、新しい脆弱性が増えたので、その内容を盛り込みました。  
  
　また、Webアプリケーションのセキュリティに関する課題解決を目的とするOWASP（The Open Web Application Security Project）という国際的なオープンなコミュニティがあるのですが、その取り組みについても盛り込みました。  
  
**石川氏：**最後に、12月4日、5日に開催される[『Canon Security Days 2018』](https://cweb.canon.jp/product/it-sec/canon-security-days2018/" \t "_blank)でご講演いただく内容について、見所を少しだけお聞かせください。  
  
**徳丸氏：**基本的なところは変わりませんが、最新のトレンドは紹介したいと思います。たとえば、つい最近、あるWebサイトでカード情報が抜かれました。  
  
　商品を購入して決済ボタンを押すと、偽の入力画面を表示して、カード情報を盗みます。しかし、ここで終わるとすぐにバレるので、エラーメッセージを出して、もう一度入力を促すメッセージを出したあと、今度は本物の入力画面に飛ばすのです。そこで正しく決済されて商品も届くので、バレにくいというわけです。こういった最新の手口についても、ご紹介したいと思います。  
  
**三輪氏：**クラウドやテレワークが当たり前になると、セキュリティの考え方も変えなければなりません。外部ベンダーに任せっきりにするのではなく、自分達のセキュリティは自分達で考えて、自らきめ細かく取り組まなければなりません。もはや、ノートPC持ち出しを禁止する時代ではありません。政府が「クラウド・バイ・デフォルト」を主張している時代なのです。  
  
　ただし、だからといって政府の方針に右にならえという単純な話ではありません。クラウドには注意すべきことが山のようにありますが、それでも得られるメリットが大きいので、政府も「クラウド・バイ・デフォルト」を主張しているのです。セミナーでは、そのあたりのお話ができればと思っています。  
  
**石川氏：**非常に楽しみなセミナーになりそうです。続きは、ぜひセミナーでお聞かせください。本日は、貴重なお話をありがとうございました。

**■Canon Security Days 2018 開催**  
標的型攻撃、マイニングマルウェア、ランサムウェアなど、サイバー攻撃が巧妙化する一方で、IoTやワークスタイル変革などの環境変化に伴い、新たなセキュリティ対策が必要になってきています。今回の『Canon Security Days 2018』では、これからのサイバーセキュリティにどのように対処すべきかをテーマに、最新の実態と対策についてご紹介いたします。品川でのセミナー開催に加え、オンラインセミナーも同日で開催いたします。  
  
**・開催日：2018年12月4日（火）・5日（水）  
・会　場：キヤノンマーケティングジャパン株式会社  
　　　　　東京都港区港南2-16-6 Canon S Tower  
・申　込：事前登録制（無料）**

[**本セミナーの詳細、お申込みはこちらから**](https://cweb.canon.jp/product/it-sec/canon-security-days2018/)

**セキュリティ戦略 ジャンルのセミナー**

* [【東京都】 11月19日 知っておきたい！新しい働き方のカタチとは](https://www.sbbit.jp/eventinfo/detail/47771)
* [【東京都】 11月20日 これが次世代のエンドポイントセキュリティ！](https://www.sbbit.jp/eventinfo/detail/47931)

[**一覧へ**](https://www.sbbit.jp/eventinfo/result.aspx?g=94)

**セキュリティ戦略 ジャンルのトピックス**

* [「Googleをお使いのあなた！」当選詐欺フィッシングはなぜなくならないのか](https://www.sbbit.jp/article/cont1/35626)
* [セキュリティ人材不足が深刻化、ガートナーはなぜ「チームの解体」を推奨するのか](https://www.sbbit.jp/article/cont1/35587)
* [なぜアドウェアは検挙されず、無断マイニングでは逮捕者が出るのか](https://www.sbbit.jp/article/cont1/35527)
* [【特集】サイバーセキュリティの心臓部](https://www.sbbit.jp/article/bitsp2/35498)
* [仮想通貨マイニング「コインハイブ」は違法？ 警察の勇み足？ 問題を整理する](https://www.sbbit.jp/article/cont1/35060)

[**一覧へ**](https://www.sbbit.jp/subcategory/94/archive/topics/1)

**セキュリティ戦略 ジャンルのIT導入支援情報**

* [立命館大 上原哲太郎教授に聞く企業セキュリティ、働き方改革と両立させるには？](https://www.sbbit.jp/article/bitsp2/35348)
* [サイバー攻撃対策は77％が「続きを考えていない」　対応だけでなく“回復”を考える](https://www.sbbit.jp/article/bitsp/35147)
* [ランサムウェアは「過去」なのか？　今なお拡大する被害に”現実的な対策”を](https://www.sbbit.jp/article/bitsp/34856)
* [2018年のサイバー攻撃はどうなる？ 名和利男×HPE 緊急対談](https://www.sbbit.jp/article/bitsp2/34460)
* [多層防御のあおりで高まる運用負荷…今こそ求められる「セキュリティ製品間の連携」](https://www.sbbit.jp/article/bitsp/34414)

[**一覧へ**](https://www.sbbit.jp/special/result.aspx?g=94)

PR

* [■米MITメディアラボ 石井裕 教授講演！IoT時代の到来、爆増するビッグデータ。東芝メモリが語るSSDの最新動向と技術戦略](https://ds.advg.jp/adpds_deliver/p/r?adpds_sid=198&adpds_fid=23416&adpds_cpn=162793&adpds_bid=467884&adpds_cid=345881&adpds_nocache=154112080089072401673&adpds_lid=1)
* [◆「データ野球」を掲げるソフトバンク。落合選手をデータで倒す？黄金時代の広島カープを知る達川光男氏が力説](https://ds.advg.jp/adpds_deliver/p/r?adpds_sid=198&adpds_fid=23417&adpds_cpn=162793&adpds_bid=467253&adpds_cid=345309&adpds_nocache=154112080114851784075&adpds_lid=1)
* [◆ ドコモ・システムズ、IT人材不足をどう解決？ 5G/IoT 時代を見据えた VMware のエッジコンピューティング戦略](https://ds.advg.jp/adpds_deliver/p/r?adpds_sid=198&adpds_fid=23418&adpds_cpn=165411&adpds_bid=468368&adpds_cid=346319&adpds_nocache=154112080132794291989&adpds_lid=1)

**[イベント・セミナー情報掲載(無料)](https://www.sbbit.jp/article/info/eventseminar)**

アクセス総合ランキング

**[1](https://www.sbbit.jp/article/cont1/35551)**

[AI・人工知能・機械学習](https://www.sbbit.jp/article/cont1/35551)

**[Windows 95の父、中島聡氏の2030年予測：経団連を見ると「GAFAに勝てるワケがない」](https://www.sbbit.jp/article/cont1/35551)**

[2018/11/01](https://www.sbbit.jp/article/cont1/35551)

**[2](https://www.sbbit.jp/article/cont1/35466)**

[ビッグデータ](https://www.sbbit.jp/article/cont1/35466)

**[データサイエンティストになるには？社内で育てる方法は？わかりやすく解説](https://www.sbbit.jp/article/cont1/35466)**

[2018/10/26](https://www.sbbit.jp/article/cont1/35466)

**[3](https://www.sbbit.jp/article/cont1/35658)**

[クラウド](https://www.sbbit.jp/article/cont1/35658)

**[IBMのRed Hat買収、MSとNECの経営陣に聞いた「評価」](https://www.sbbit.jp/article/cont1/35658)**

[2018/11/01](https://www.sbbit.jp/article/cont1/35658)

**[4](https://www.sbbit.jp/article/cont1/35587)**

[セキュリティ戦略](https://www.sbbit.jp/article/cont1/35587)

**[セキュリティ人材不足が深刻化、ガートナーはなぜ「チームの解体」を推奨するのか](https://www.sbbit.jp/article/cont1/35587)**

[2018/10/30](https://www.sbbit.jp/article/cont1/35587)

**[5](https://www.sbbit.jp/article/cont1/35575)**

[ロボティクス・ドローン](https://www.sbbit.jp/article/cont1/35575)

**[【全20ジャンル総覧】国内ロボット業界の「量産化」動向を徹底分析](https://www.sbbit.jp/article/cont1/35575)**

[2018/10/30](https://www.sbbit.jp/article/cont1/35575)

注目のイベント・セミナーランキング

**[東京都2018/11/30開催](https://www.sbbit.jp/eventinfo/detail/47664)**

**[1](https://www.sbbit.jp/eventinfo/detail/47664)**

**[東芝メモリ SSDフォーラム 2018](https://www.sbbit.jp/eventinfo/detail/47664)**

**[東京都2018/11/13開催](https://www.sbbit.jp/eventinfo/detail/47236)**

**[2](https://www.sbbit.jp/eventinfo/detail/47236)**

**[ウイングアークフォーラム 2018 ［東京］](https://www.sbbit.jp/eventinfo/detail/47236)**

**[東京都2018/11/30開催](https://www.sbbit.jp/eventinfo/detail/47823)**

**[3](https://www.sbbit.jp/eventinfo/detail/47823)**

**[IBM Cloud ＆ AI Conference](https://www.sbbit.jp/eventinfo/detail/47823)**

**[東京都2018/11/08開催](https://www.sbbit.jp/eventinfo/detail/47592)**

**[4](https://www.sbbit.jp/eventinfo/detail/47592)**

**[RED HAT FORUM Tokyo 2018](https://www.sbbit.jp/eventinfo/detail/47592)**

**[東京都2018/11/22開催](https://www.sbbit.jp/eventinfo/detail/47697)**

**[5](https://www.sbbit.jp/eventinfo/detail/47697)**

**[未来を拓くアプリケーション、メッセージング基盤](https://www.sbbit.jp/eventinfo/detail/47697)**