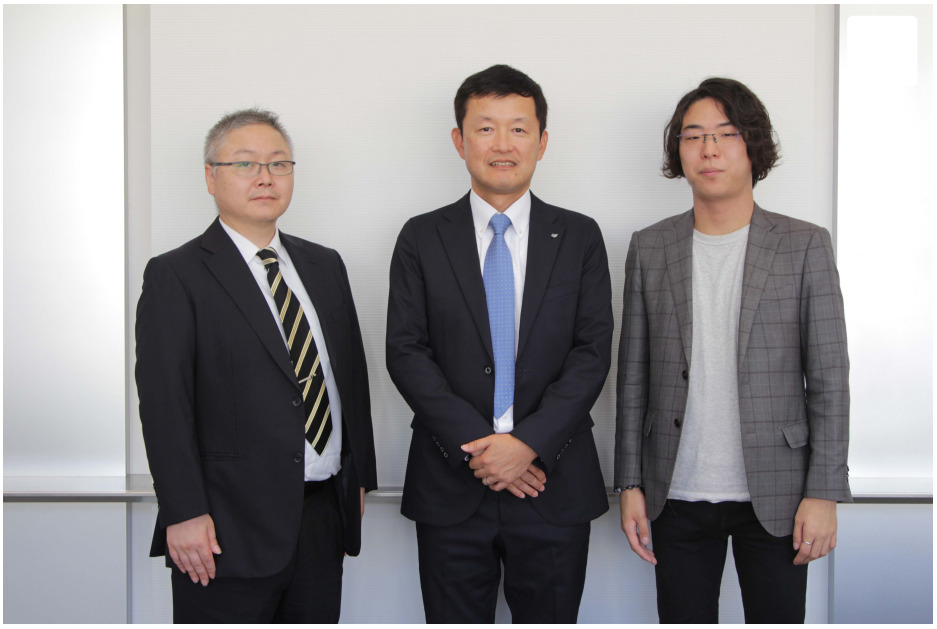
関連ジャンル セキュリティ戦略 クラウド 情報漏えい対策 セキュリティ総論
キヤノンマーケティングジャパン株式会社提供コンテンツ スペシャル 2019/10/23

【鼎談】DX時代のセキュリティは「NIST」に対応しなければ始まらない

西尾素己氏×洞田慎一氏×石川滋人氏 対談

現在、多くの企業が「デジタル・トランスフォーメーション（DX）」に取り組んでいる。ここで見落としてはならないのが「セキュリティ」対策だ。そこで「DX時代に求められるセキュリティ」をテーマに、多摩大学 ルール形成戦略研究所首席研究員の西尾素己氏、JPCERTコーディネーションセンター早期警戒グループ担当部門長 兼マネージャ、サイバーメトリクスグループ部門長 兼 マネージャの洞田慎一氏が対談した。ファシリテーターは、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事業企画部 部長の石川滋人氏が務めた。



JPCERTコーディネーションセンター 早期警戒グループ 担当部門長 兼 マネージャ サイバーメトリクスグループ部門長 兼 マネージャ　洞田慎一氏（左）、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事業企画部 部長 石川滋人氏（中）、多摩大学 ルール形成戦略研究所首席研究員 西尾素己氏（右）

DXで避けられない3つのポイント

石川氏：まずは、デジタル・トランスフォーメーション（DX）と企業ITの関係から議論を始めたいと思います。切り口はいくつかあると思います。

1つが、経済産業省のDXレポートが発端となった「2025年の崖」問題です。同レポートでは「企業が保有するレガシーシステムを放置すると、2025年以降、年間約12兆円もの経済的損失がある」と警鐘を鳴らしています。

2つ目は「デジタルを活かしてビジネスをいかに変革していくか」という視点です。そして3つ目が、DXを推進していくにあたり、いかにしてセキュリティを確保していくかということです。

西尾氏：1つ目のレガシーシステムに関しては、新しい基盤にシステムをのせてしっかりとメンテナンスすることがセキュリティの担保につながります。そもそも基盤が古いままだと、新しいテクノロジーが出てきても活用できません。

2つ目のデジタルなビジネス変革のキーワードは「IoT（Internet of Things）」や「IoE（Internet of Everything）」です。たとえば、電柱にセンサーを付けて、その情報を使って自動車事故を防ぐような取り組みが出てきています。このように、非ITだった領域がIT化していくと、そこでのセキュリティの担保が求められます。米国ではいち早く法律で対応しようとしています。

多摩大学 ルール形成戦略研究所首席研究員 西尾素己氏

洞田氏：レガシーなシステムをなくそうとすることだけに固執することはないのだと思います。現実問題として、数十年前に開発されたプログラムが今もどこかで動いていて、それが正しく機能していることは否定できないでしょう。たとえば、目の前にインターネットが普及する以前から使われているPCやメインフレームがあって、何の問題もなく業務ができているとします。それ自体がなにか不具合があるということではなく、問題となるのは、それをネットワークに接続して使ったとき、それはセキュリティに対してどのような問題を与えるのか。レガシーかどうかを問うことではなく、より重要なことは「他システムと組み合わせて使ったとき、その影響を正しく認識できているかどうか」です。

次世代通信規格「5G」の普及を阻む、大国間の深い溝

石川氏：DXを推進するうえでは、商用化が見込まれている次世代移動通信の「5G」技術もかなり重要な要素です。

西尾氏：5Gのメリットの1つが「高速大容量」である点です。IoTやクラウドとの接続スピードが格段に速くなります。また「同時接続性」「低遅延通信」などもメリットとして挙げられます。たとえば、高速道路を自動運転車が走っていて、100メートル前の車が急ブレーキをかけたとします。それが後続車に伝わるのに2、3秒もかかっていたら、とても自動運転は実現できません。したがって、商用利用ではかなり盛り上がると思います。

石川氏：IoTとクラウドに5Gは不可欠ということですね。一方で5Gの通信基盤を整備していく上では技術面でも政策面でもまだまだ課題があるように思います。

西尾氏：以前、安全保障のテーマとして5Gを研究したことがあります。5Gでは、ほとんどの基礎技術を中国企業が押さえています。それは通信規格ではなく、よりプリミティブなアンテナの技術です。5Gを実現するには「Massive MIMO（マッシブ マイモ）」というアンテナが不可欠なのですが、そのほとんどが中国企業の特許技術なのです。

約2年前、米国でこの問題が議論されました。世界中の基地局に中国製の機器が入ったネットワークが構築されるわけですから、安全保障の関係で問題視されたのです。しかも、明らかにバックドアと思われるコードが発見されたという数多くの研究結果が存在します 。では、中国企業の技術を使わないで5Gが実現できるかというと、それも難しいのが実情です。どうしても性能が劣ってしまうのです。

当時、米国は「イノベーションか、安全か」を問われていたのです。結局、同国は中国企業の技術を使うしかないとなりかけました。ところが、2018年8月に米国で成立した「国防権限法2019」では、中国企業5社を米国の政府調達から閉め出すことを決めました。不透明感が増しているのです。このような米国の流れは米国の国内法の整備により、サプライチェーンへのフローダウンという形で世界中に影響を及ぼします。

ユーザーの想定外の行動にどう対応する？

石川氏：DXによりクラウドの積極活用などITインフラ環境が大きく変化すると、“情報の流れ”が変わり、従来のセキュリティポリシーや運用管理ではセキュリティの担保が困難になると思います。長年、セキュリティインシデントを見てきた洞田さんはどうお感じでしょうか。

洞田氏：経産省が提案する「サイバー・フィジカル・セキュリティ対策フレームワーク」でも触れられていますが、今後サイバー空間とフィジカル空間での企業やユーザーの活動が拡大することで生まれる注意点があると思います。たとえば、ユーザーが自由にデータを活用して処理していく過程で、そのデータや機器を提供するメーカー側が意図しない使われ方が生まれる可能性が1つには考えられます。ちょうど3Dプリンタが登場し、開発側が予想していなかった使われ方が生まれたのに似ています。その際、企業側は「そうした使われ方は想定していなかった」と言えるのかどうか。十分に注意しておく必要があると思います。

JPCERTコーディネーションセンター　早期警戒グループ 担当部門長 兼 マネージャ サイバーメトリクスグループ部門長 兼 マネージャ 洞田慎一氏

西尾氏：今のお話を聞いて、AI（人工知能）を連想しました。現在、倫理面も含めたAIの使い方が世界的な議論になっています。DXが進むと、これまでは集めていなかった膨大なデータも収集することになります。それを人が処理するのは現実的ではないため、AIのようなエンジンが処理することになります。その際、どのようなAI利用が適法で、どういうAI利用がグレー、もしくは違法なのかが議論されています。

　たとえば、ある就職情報サイトが内定辞退率のデータを企業に販売して大きな問題となりました。内定辞退率のような人の気持ち、思いのようなものを、そもそもAIで数値化して良いのかということですね。さらに集めたデータの中に個人情報に当たる情報があるのか否かについても重要な観点になります。直接的な個人情報でなくとも家電製品の稼働状況など間接的にその人の行動などをトレースできる情報についても注意する必要があります。

石川氏：日本企業は個人情報の取り扱いには敏感です。規模は違いますが、GDPR（一般データ保護規則）もその延長線上で考えられるでしょう。ただし、AIに関して

は異なったアプローチが必要になるでしょう。

洞田氏：AIでは処理される情報には、いわゆる個人情報以外の情報も含まれていると考えられます。それらのデータをどのように管理・整理しておくかが重要であることは言うまでもありません。加えて、それぞれの個々の情報やその取扱いに問題がなかったとしても、AIで処理された上で生まれる「二次生成物」をどう扱うのかも、企業が整理しておくべき重要な課題です。

サプライチェーンのセキュリティ確保と米国の動向

石川氏：サイバー攻撃はますます巧妙化していますが、最近の傾向をお聞かせください。また、サプライチェーンにおけるセキュリティについても現状を解説していただけますか。

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事業企画部 部長
石川滋人氏

洞田氏：使われる技術、脆弱性、ツールなどは変化していますが、サイバー攻撃の狙いや考え方そのものは、著しく変化したとまでは言えないと思います。たとえば、同じような攻撃が発生し、順番に対策の手薄なところが狙われているように見えるものもあります。このことは、サイバー攻撃に備えるとしても、何から手を付けたらよいかわからない、という状態のままの組織がまだ残されているのではないかとも考えられます。

サプライチェーンのセキュリティを考えた場合、チェーンの中にはそうした手薄な組織が残っている可能性も考えられ、全体としてインシデントの影響を受ける可能性を考えるのが望ましいのではないかと思います。場合によっては、複数社が関係する場合のインシデントに対しても巻き込まれるケースも考えられます。関係企業から「これは御社の問題ですね」と問われたとき、正しい技術情報に基づく事実を客観的に説明できることが求められるでしょう。加えて、お互いにセキュリティに関してフェアに話ができるかどうかも大切ですね。

西尾氏：2010年以降、米国ではサイバー攻撃による被害、知的財産の盗用といった事案が増えました。これに関連して裁判が起き、企業側のセキュリティが十分であったかどうかが重要な争点となりました。しかし、そのたびに専門家が出てきて「こういう対策をしていたが避けられなかった」といった説明を繰り返しました。

ところが、その内容が会議や専門家によって変わるケースが相次いだのです。このため、陪審員の印象によって判決が変わる状況が生まれました。これでは、法の下の平等が保たれません。

そこで法曹界を中心に「ITの素人である自分たちにも判断できる仕組みを作るべきだ」という動きが起きました。その1つが「NIST SP800」のフレームワークです。Controlled Unclassified Information（CUI）と呼ばれる情報を扱うにはこのフレームワークに準拠していることが最低条件になります。これがあれば、仮に悪意ある攻撃によって被害が発生しても、企業側がフレームワークに準拠していたことが証明できれば責任を問われません。逆に証明できなければ、責任を問われることになるわけです。今さまざまな業界でこのフレームワークが採用されています。これは米国のサイバー攻撃対策における企業側の明らかな過失責任を問うためのものだと言えます。

日本企業のNIST対応は30%～50%、ISMSとは別物という認識が必要

石川氏：サプライチェーンのセキュリティを確保していく意味でも、自社の正当性を示す意味でもセキュリティ対策の基準が必要ということですね。その基準となる「NIST SP800」のフレームワークについて詳しく教えてください。

西尾氏：たとえば、米国の国防総省（DoD）が戦闘機を開発するとき、その設計図は当然、同盟国である日本企業にも渡りますし、その下請け企業でも設計図を扱うことになります。米国の安全保障にとって非常に機微な情報ですから、NISTのフレームワークに従うことが求められます。つまり、米国の政府組織と何らかの取引のある日本企業は、事実上、NISTのフレームワークに対応しなければなりません。これはDFARS 252.204-7012で規定されており、連邦調達規則（FAR）52.204-21や32 連邦規則（CFR）2002.14により、すべての産業が対応を求められるのが、2020年です。

こうした安全保障を“テコ”にして経済政策を進めようとする概念を「エコノミック・ステートクラフト（Economic Statecraft）」と呼びます。安全保障に関する用語ですが、日本語では「安全保障経済政策」と訳します。

石川氏：日本企業は、現時点でNISTのフレームワークにどの程度対応できているのでしょうか。

西尾氏：はっきり申し上げて、まったく不十分です。ここ数年で十数社をヒアリングしましたが、30%～50%程度で止まっている印象です。ただ、幸いなことに日本企業は「情報セキュリティマネジメントシステム（ISMS）」への対応は進んでいます。そのため、ISMSへの対応をベースにNIST対応を進められるメリットはあります。

ただし、両者は根本的に別のものです。最大の違いは、NISTが「特定」「防御」「検知」「対応」「復旧」という5段階を考えるのに対し、ISMSは特定と防御を注視していることです。これはISMSが管理基準でありサイバー攻撃に技術的に対抗するためのフレームワークではないからです。さらに、NISTには技術的な強度の指定があります。たとえば、ISMSでは暗号化は求められていますが、その技術までは指定されていません。一方、NISTでは暗号化の技術まで指定しています。

石川氏：ご指摘の通り、ISMS対応がなされているとNISTにも対応できると錯覚しがちですね。NIST対応を進める上での重要なポイントの1つになりそうです。

自主基準に任せている現状、急がれるルールの整備

石川氏：セキュリティは一朝一夕ではできるものではありません。インシデントと格闘しながら、試行錯誤で積み重ねていくものだろうと思います。その意味では、DXによってセキュリティ対応できる企業とそうでない企業の二極化が起きるという懸念はありませんか。

洞田氏：たとえDXが進んだとしても、すべての業種で形態が変わるとは言えないと思います。加工や処理の精度、品質を極めていくことが組織としても業界としても求められる企業は、やはりその価値観を中心においた活動を展開するのだと思いますし、それがDXで変わるということではないと思います。もちろんそのプロセスにおいてDXにより変化するものはあるとは思います。

その中で考えないといけないことは、それぞれの企業の単独の活動ということだけではなく、西尾さんが戦闘機の例で指摘したように、国内企業であっても、どこかで海外のサプライチェーンの一部に組み込まれていれば、その影響を受ける可能性が考えられます。それにどのように、またどこまで取り組んだらよいかという課題は、今現在は各企業や業界の自主基準に委ねられているのだと感じます。その意味でも企業はさまざまなフレームワークに留意する必要があり、NISTのフレームワークもその1つとして企業は留意しておく必要性がでてくるのだと思います。

西尾氏：たとえば、複合機やプロジェクターなどのOA機器であっても、ネットワークでシステムとつながっていればNIST対応の対象になります。すでにNIST対応をうたう製品も登場していますが、今後はこうしたOA機器などの分野でも、NIST対応の製品が数多く出てくると思います。こうした製品調達のような日々の業務からでもNIST対応が開始できることは、ぜひ強調しておきたいですね。

石川氏：DX時代にセキュリティ変革を進めていく上でのポイントは、正しい技術情報と脆弱性情報をタイムリーに収集し、対処をしていきながら、NIST対応を確実に進めていくことが重要だということですね。DXとセキュリティ対策の関係性は、各企業が真剣に向き合い、考えるべきテーマであることは間違いなさそうです。

西尾様と洞田様には、11月12～13日に開催される「Canon Security Days / ESET Security Days 2019」のパネルディスカッションにも登壇していただく予定です。さらに詳しいお話をお聞かせいただけるのを楽しみにしております。本日は貴重なお話をありがとうございました。

セキュリティ戦略 ジャンルのセミナー

- 【東京都】 11月6日 AIセキュリティセミナー
- 【東京都】 11月28日 サイバーセキュリティ対策セミナー2019 冬
- 【東京都】 11月29日 Citrix Future of Work Tour

▸ 一覧へ

セキュリティ戦略 ジャンルのトピックス

- ゼロトラストセキュリティとは何か？ そのアーキテクチャと運用体制

- なぜ「諜報活動を教える大学」が増えているのか？ 学生人気も急上昇
- GAFAでも独特なアップルのセキュリティ戦略、サブスク参入で変わってしまうのか
- サイバーレジリエンスとは？ 定義や手法、体制の作り方を解説
- ネット犯罪対策キーマンが警鐘、「Facebookで誘導する」ダークウェブの危険

▸ 一覧へ

セキュリティ戦略 ジャンルのIT導入支援情報

- 相次ぐ「情報漏えい」「不正アクセス」、次はあなたの会社かも
- 宅ふぁいる便のパスワード漏えいは他人事か？2019年サイバー攻撃のトレンドとその対策
- 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」
- 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？
- 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

▸ 一覧へ