IIJ.news

IIJ was founded in 1992 as a pioneer in the commercial Internet market in Japan. Since that time, the company has continued to take the initiative in the network technology field, playing a leading role in Japan's Internet industry. The history of IIJ is indeed the history of the Internet in Japan.

December 2026

VOL. 197

特集

AI時代のサイバーセキュリティ

――“守っているつもり”を問い直す



IIJ. news
December 2026
VOL. 197



3 ぷろろーぐ めざめ／鈴木 幸一

4 Topics
AI時代のサイバーセキュリティ
——“守っているつもり”を問い直す

6 そのリスク、誰が拾いますか？——3線モデルの隙間を埋める「第4の網」／加賀 康之
10 攻撃者から見た貴社のシステム——AI時代に見直したい「外からどう見えているか？」という視点／鳥山 悟
14 自社の備えを、今一度、確かめてみませんか／小宅 洋光

18 IIJ Research となりの情シス 全国情シス実態調査 2026
20 人と空気とインターネット 自分の目で見て、手で触れながら考える／浅羽 登志也
22 Technical Now 教育・研究を支える情報基盤をリプレース
24 インターネット・トリビア 脆弱性アップデートはなぜ「予告」されるのか？／堂前 清隆
25 Information
26 パラフェンシング笹島貴明の“Allez（アレ）”！／笹島 貴明
表紙の言葉 編集後記

ぷろろーぐ

めざめ

株式会社インターネットイニシアティブ
代表取締役 会長執行役員
鈴木 幸一

幼い頃から早起きで、家族からうるさがられた挙げ句、朝起きると、枕元におにぎりか、何か食べられるものが置いてあって、それを食べることで、家族に迷惑をかけないようにされていた。

その習慣は大人になっても変わらず、睡眠時間が短く、夜明け前の四時頃には目を覚まし、ウロウロと年齢に応じた夜明け前の活動をしていたのだが、ここ四、五年は、年齢を重ねたせいか、夜明け前の過ごし方が変わってきてしまったようだ。昔から、横になったまま、よろず思いを巡らすこともなく、すぐに寝床から出てしまう習性は変わりないのだが、その後、夜明けまでの時間の過ごし方が、怠惰になってしまっているのだ。

目覚めて、まずコーヒーを淹れる。変わらないのはそこまでで、コーヒーの飲み方から違ってしまっている。本を読むことが、すべてに優先していた私は、淹れたコーヒーを手に、机に座って、本や資料を読む、あるいは、ぼんやりと肘をついて、何かを考えている風にしていたのだが、最近は、コーヒーカップを手に、すぐにソファに座り込んで、ぼんやりしている時間が年ごとに長くなっている気がする。秋になり、夜明けが遅くなっているのに、長いことソファに座って、何事か考えているような姿のまま、夜明けを待っているのである。ネットをつなぐと、世界のあらゆるニュースを眺めることができるのだが、それもしない。読む時間を見つけられずに、本棚に置いたままになっているたくさんの書物を手にすることもない。別段、ボケが進んでいるわけでもないと思うのだが、夜明けの時間の過ごし方が退化して、何もしていない時間になっているのである。

毎夜、酒席が続いて、朝になっても疲れがとれないのではと、知人は言ってくれるのだが、そうでもない気がする。高齢者の仲間入りをしても、私の酒量は落ちていない。年齢を重ねることで、体力、知力、気力など、あらゆる活動を促す内的なエネルギーが小さくなっていくのかと思うのだが、衰えが目立つことと、そうでもないことがはっきりしてくるようだ。

まず老いを感じるのは、ゴルフの飛距離と記憶力のような気がする。記憶力については、ネットの利用によって、身近なところではスマホ依存が進み、脳の記憶容量が小さくなってしまったようだ。子供もネット利用が進むにつれて、記憶を左右する脳の容量が小さくなってしまうという警告は、何年も前から海外の研究者から出されていて、子供の使用を禁止する国も出ているのだが、日本では大きな議論になっていない。小学校にあがる前の年齢で、スマホに記憶を依存するようになるのはいかがなものかと思うのだが。大きな技術革新は、人間のありようそのものを変えてしまうのである。

四〇年近く、その技術革新を普及させ、利用できるように、世界に後れをとらない国にしようとしたことが、私の後半生の仕事になったのは、皮肉といえば皮肉な話である。



イラスト／末房志野

TOPICS

AI時代のサイバーセキュリティ
――“守っているつもり”を問い直す

生成AIの登場によって、サイバーセキュリティのあり方が変化し始めています。AIは攻撃者の情報収集、フィッシング文面の作成、脆弱性の探索などを効率化し、従来の攻撃をより速く大規模に実行しやすくしています。一方、企業側でもAIの業務利用が広がり、入力情報やサービス管理、利用ルールの整備といった課題が生じています。

2026年のサイバーセキュリティを取り巻く状況を振り返ると、新しい脅威だけでなく、ランサムウェア、認証情報を狙うフィッシング、既知の脆弱性や設定ミスの悪用、サプライチェーンを経由した侵入など、以前からある攻撃が形を変えながら続いていることがわかります。

企業のIT環境も変化しています。クラウドサービスの利用が一般化し、自社のシステムが、委託先や取引先、外部サービスと密接につながるようになるなか、守るべき範囲は社内だけに限られません。攻撃者は、厳重に守られた重要システムへ正面から侵入を試みるより、外部の公開資産、アカウント、VPN、委託先、開発環境など、侵入が容易な経路を常に探しています。

ランサムウェアも、ファイルを暗号化して身代金を要求するだけの攻撃ではなくなっています。機微情報を窃取し、その公開を材料に金銭を要求するなど、事業や社会的信頼に影響を及ぼすような手口も増えています。そのため、バックアップや境界防御に加え、異常の早期検知、被害範囲の限定、関係者への報告・説明、重要業務の復旧までを含めた備えが必要です。

変化するリスクに対応するには、新しい製品を追加するだけでは十分でなく、自社にとって重要な業務と情報を把握し、現場・リスク管理部門・内部監査部門・経営層が連携して優先順位を判断すること、導入した対策が日々の運用や問題発生時にきちんと機能するかを継続的に確かめることが必須です。

本特集では、組織を横断してリスクを捉える方法、攻撃者から見た多様な侵入経路、チェックリストを使った備えの点検などを取り上げます。組織・技術・運用の3つの面から、これからのセキュリティについて考える契機になれば幸いです。

イラスト／もんくみこ

そのリスク、誰が拾いますか？
――3線モデルの隙間を埋める「第4の網」

生成AIの台頭とともに、サイバーセキュリティも変革を余儀なくされている。本稿では、内部監査団体（IIA）が提唱する、組織のガバナンスとリスク管理に関するフレームワーク「3線モデル」をベースに、新たな時代に即したセキュリティのあり方を考える。

IIJ ネットワークサービス事業本部 セキュリティ本部 セキュリティビジネス推進部長
加賀 康之

ランサムウェア対策、大丈夫？

突然ですが、ランサムウェア対策、完了しましたか？「実装完了して運用を開始した」という企業もあれば、「今、まさに実装中」といったところも多いのではないでしょうか。

ランサムウェア対策と言えば「バックアップ」です。バックアップ製品の選定・構築、バックアップ対象システムの選定、運用設計、発動時のランスルーテスト……ここまでやって、ようやくカットオーバーです。お疲れさまでした。「これで我が社もランサムウェア対策完了！」と言いたくなるかもしれませんが、そうは問屋が卸さないのが、サイバーセキュリティ対策のむずかしいところです。

ランサムウェア対策はバックアップシステムの導入・構築、運用だけではありません。いざランサムウェアに感染すると――

- システムの暗号化
- システムの停止
- 顧客説明
- 対外発表
- 記者会見
- 監督官庁への報告
- 損害賠償
- 株価低下
- ブランドイメージ低下
- 連日の役員会議
- 社員の通常業務停止

これらへの早急な対応が求められますが、バックアップで保護できるのは最初の二つだけです。その他の項目を「いつ・誰が・どうするのか」決めていますか？

時々、ランサムウェアをBCP対策の延長で語る方がいらっしゃいます。たしかにシステム的対応は、BCP対策に近いところはありますが、通常のBCP対策（首都直下型地震、南海トラフ地震、富士山噴火など）とは発生のシチュエーションが違うことを念頭に置く必要があります。大規模地震などの災害は、周りも少なからず同じ被害を受けていたり、仮に受けていなくても「災害だからしょうがないね」と同情してもらえるかもしれません。

一方、ランサムウェア被害は自社に限られ、周りの経済活動は動いたままです。顧客は来るし、物流は動いているし、競合他社は商売を続けています。そうなると、やるべきことは同じでも、優先順位が異なります。迅速なシステム復旧は言うまでもなく、顧客説明、対外発表、監督官庁への報告は一刻をあらそいます。

自然災害の場合、ブランドイメージの低下や損害賠償といったリスクは低いかもしれませんが、「うちはBCP対策はできているから、ランサムウェア対策も大丈夫」という考えは少々危険かもしれません。

全部準備するのは無理！

全てに対応するのは無理ですよね？わかります。しかし、全てを完璧に準備しておかなくても、「セキュリティ対策は受容する」という究極の選択肢があります。「受容する」とは、リスクを無視するということではありませんし、認識して受け入れるということでもありません。

リスクマネジメントにおける「受容」は、リスクを正しく評価し、発生確率を鑑み、事業継続性と対策コストを比較して、経営層がリスクを引き受ける判断をすることです。日本企業にありがちな、幹部社員だけの会議で「このリスクは残ってしまう。でも誰がやるの？簡単には対策できないから、いったん課題として置いておきますか」――こういったことは〝会議あるある〟かもしれませんが、「受容」とは言いません。「放置」です。「受容」とは経営層が正しく理解し、経営判断としてリスクを引き受けることを指します。

だからと言って「あふれる対応は全て経営判断してください」では、経営層はたまったものではありません。そもそも部下から判断できる材料が上がってこないことが多いのが実情です。

IIAの「3線モデル」とは

そういった状況下で、リスク管理部門の担当者、幹部社員が迅速かつ正確に現状を報告し、経営層が正しい判断ができるようにするための態勢作りのフレームワークとして「3線モデル」（Three Lines Model）があります。

3線モデルは、米国に拠点を置く国際的な内部監査団体「The Institute of Internal Auditors」（IIA）が二〇一三年に公表した「Three Lines of Defense」（三つの防衛線）というポジションペーパーに由来します。

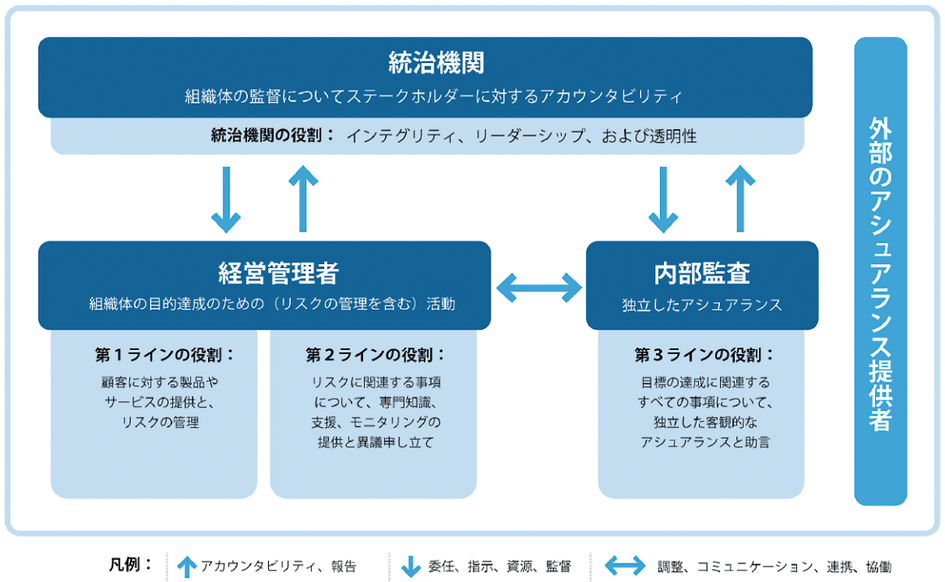
3線モデルの基本的な考え方は「第1線は事業部門（現場）」、「第2線はリスク管理部門」、「第3線は内部監査部門」とし、二〇一三年版では「現場部門・リスク管理部門・内部監査部門」を三つの防衛線として整理し、防御的なリスク管理に主眼が置かれていました。

そして二〇二〇年、IIAはこれを「Three Lines Model」に改訂しました。ここでは、従来の三本の防衛線という考え方から一歩進んで、3線とガバナンス、マネジメントが相互に連携する形に再整理されました。このフレームワークを用いてリスク管理体制を構築している企業も多数あると思います。

ちなみに、この「1線、2線、3線」と「防御」といった言葉から、右図のような縦の主従関係をイメージされるかもしれませんが、IIAが示すモデルはまったく異なります（下図参照）。

1線 事業部門（現場）
▼
2線 リスク管理部門
▼
3線 内部監査部門

IIAの 3ラインモデル



©2026, The Institute of Internal Auditors, Inc. Used by permission. All rights reserved.
出典：IIA「3ラインモデル」https://www.iiajapan.com/leg/pdf/data/iia/2020.07_1_Three-Lines-Model-Updated-Japanese.pdf

IIAのモデルにおける各線（ライン）は、組織の上下関係を表すものではありません。また、番号は業務の順序を示すのではなく、全ての役割は同時に行なわれる、と明記されています。

3線モデルが足かせになる？

筆者は日頃の業務を通じて、さまざまな立場の方々とお会いします。インシデント対応の現場では、まさに1線にあたる担当者に話をうかがいます。時にはセキュリティ事故を起こしてしまった新人社員にヒアリングすることもあります。

CISO（Chief Information Security Officer）やCISO補佐といった経営幹部の方とリスク管理について議論する機会も少なくありません。そのなかには1線、2線、3線を、明確に組織や役割に紐づけて運用している企業も多いのですが、そうした方々とお話していると、ごくまれに「おや？」と思う場面に出会います。

以前、2線の担当者と技術的な話をした際、「私は2線なので、○○は1線の人が理解していればいいですよね」とおっしゃいました。一方、別の企業で今度は、1線の方に○○を利用するうえでのガイドラインはあるのか尋ねると、「それは2線が方針を決めてからです」という答えが返ってきました。

「……おや？」

先に書いた通り、3線モデルは組織全体でリスク全体を管理するフレームワークであり、全ての役割は同時に行なわれるはずです。1線は方針を考えなくてよく、2線は技術を知らなくていいわけではありません。むしろ2線は技術を理解したうえで、運用に沿った方針を出すべきであり、1線は使い方をきちんとフィードバックし、生産性とセキュリティを両立させながら業務を遂行すべきです。それを行なわなければ、誰にも参照されないガイドラインや規定が作られ、SaaSのグレーな使われ方が横行する結果を招いてしまいます。

では、どうすればいいのでしょうか？3線モデルが悪いわけではありません。正確に理解し、適切に運用すれば、組織全体のリスク対策向上につながることは間違いありません。役割と組織を紐づけるのもわかります。運用しやすいですよね。組織のミッションとリンクさせやすい。メンバーの目標に反映しやすい。要は、業務に組み込みやすいわけです。しかしそうなると、「それは1線の仕事だから……」、「それは2線が方針を決めたあとでやります」、「3線のレビューが終わってから考えます」といった具合に、いつの間にか組織のあいだに〝壁〟を作る一因となってしまい、これでは本末転倒です。

〝隙間に落ちたリスク〟を見過ごさない

少し話が変わりますが、今日、私たちは大きな変革のなかにいます。筆者はこの業界に三〇年ほどおりますが、その間、これは大きな変革だなと感じたことが何度かありました。古くはインターネット常時接続の開始、スマートフォンの登場、クラウドシフトなどです。

しかし、ここ数年の生成AIの台頭は、これまでとは次元が違うレベルでの変革だと感じています。業務の効率化、生産性の向上だけではありません。例えば、子どもたちは親ではなく生成AIに相談し、資産運用のアドバイスもAIが行ない、もしかすると役員も昔は部下に聞いていたことを今は生成AIに聞いているかもしれませんね。日々の暮らしというより、人生設計にまでAIが関わる時代がすぐそこまで来ているのです。



そんな時代にサイバーセキュリティ、リスク管理も変わらないわけがありません。数年前に1線、2線、3線と決めた業務範囲がすでに旧態化していてもおかしくありません。サイバーセキュリティ対策は状況に即したバージョンアップを行なうと同時に〝隙間に落ちたリスク〟を見過ごさないことが大切です。

生成AIセキュリティ

AIの話題が出たので、近年、まさに〝隙間に落ちたリスク〟の筆頭と言える「AIセキュリティ」に触れたいと思います。

お客さまとAIセキュリティについてお話しすると、「入力した情報は漏れませんか？」という質問がもっとも多く寄せられます。この「漏れませんか？」という意味は大きく三つに分類されます。

- 学習に使われる
- サービス提供ベンダの開発者が読む
- ログとして保存される

これらについては、AIサービス提供側の利用規約やプライバシーポリシーに明記されていることがほとんどです。

例えば「学習に使われる」については、OpenAIのChatGPT「Privacy and policies」*に次のような記載があります。

When you use our services for individuals such as ChatGPT and Codex, we may use your content to train our models.

（ChatGPTやCodexなどの個人向けサービスをご利用いただく場合、お客さまのコンテンツを使用して当社のモデルをトレーニングすることがあります）

二つ目の「開発者が読む」については、Google のGemini Apps Help に次のような記載があります。

A subset of chats are reviewed by human reviewers (including Google's trained service providers) to help improve Google services.

（チャットの一部は、Google サービスの改善に役立てるため、人間のレビュー担当者［Google の訓練を受けたサービスプロバイダを含む］によってレビューされます）

三つ目の「ログとして保存される」については、次のような記載があります。

Reviewed chats are retained for up to three years.

（レビュー済みのチャットは最長で三年間、保存されます）

これは全てのセキュリティ対策製品に言えることですが、AIセキュリティ製品を導入する前に、まずは自社の従業員に許可しているAIサービスの規約を確認・把握することが先決です。それでもまだ不安要素があったり、AIサービス提供者の回答が曖昧でリスクが残っていれば、「自社で必要なAIセキュリティ対策は何？」、「そのリスクを低減できる技術・製品は何？」を選定したうえで、導入することが大事です。

〝隙間に落ちたリスク〟を救う「リスク発見会議」

AIセキュリティは〝隙間に落ちたリスク〟の一例に過ぎません。新しい技術、新しいサービス、新しい規制ができたタイミングで新たなリスクが生まれます。「1線がセキュリティ製品を検討しているだろう」、「2線のガイドラインが出るのを待とう」などとお見合いしている場合ではありません。「気が付いた人が率先してやればいい」ということでもない。気づいた人任せにすると、技術に強い人、興味がある人に仕事が偏り、属人化を助長してしまいます。現代の仕事のスタイルにも合いません。

筆者が提案するのは、CISOを中心に1線、2線、3線を混ぜた「第4の網」を設けることです。そこでは「相手の意見を否定することなく」、「忌憚のない意見交換を行ない」、「誰が担当するのかまでは決めなくてよい」。そのうえで、左記の事柄を実行します。

①発見：こんなサービスが使われ始めている
②言語化：こういうリスクがありそうだ
③一覧化：CISOなどリスクを判断する立場が把握できる状態にする

この集まりを名付けるなら「リスク発見会議」とでも言いましょうか。重要なのは「第4の網」は「4線」を作るという意味ではない点です。新しい部門を作れば、今度はそこが新たにサイロ化してしまいます。そうではなく、1線、2線、3線を横断しつつ、どの線にもまだ落ちていないリスクを拾うために「網」を張るのです。

誰の仕事かを決める前に、まず「誰も知らないリスク」をなくしていくことが、生成AI時代に必要なリスク管理ではないかと考えます。

＊How your data is used to improve model performance | OpenAI Help Center
2026年9月現在。ここにはオプトアウトする方法も記載されている。

攻撃者から見た貴社のシステム
――AI時代に見直したい「外からどう見えているか？」という視点

ランサムウェアや情報漏えいのニュースを見るたびに「なぜ侵入を許したのか？」と思う向きも多いかもしれないが、攻撃者は直接、本丸を狙うのではなく、〝もっとも入りやすい侵入口〟を探している！本稿では「貴社のシステムは、外からどう見えているか？」という視点から、AI時代のセキュリティ体制を再検討する。

IIJ ネットワークサービス事業本部 セキュリティ本部 セキュリティビジネス推進部 インテグレーション課
鳥山 悟

重要なシステムがどれほど厳重に守られていても、その周辺に弱点があれば、攻撃者はそこを足掛かりに侵入を試みます。近年は単純なフィッシングだけでなく、認証情報の窃取やサプライチェーン侵害など、多様な経路が利用されています。

さらにAIの普及によって、この状況は大きく変わりつつあります。AIが新しい攻撃手法を生み出すことに加え、攻撃者の情報収集や攻撃準備、侵害後活動を高速化・自動化し、少人数でもより多くの標的を攻撃できるようになっています。

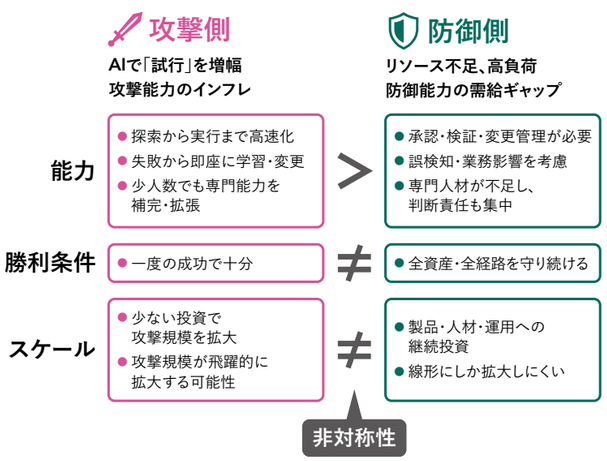
AI時代に拡大する攻撃と防御の非対称性

サイバーセキュリティの本質の一つに、攻撃者と防御側の〝非対称性〟があります。攻撃者は攻撃を試みた数千社のうち一社でも侵害できれば利益を得られますが、防御側は多様なシステムや利用者を常時、守らなければなりません。

また、防御側は人材・監視運用・脆弱性管理・インシデント対応・セキュリティ投資などを継続的に拡充する必要があります。一方、攻撃側では分業化やサービス化が進み、必要な作業をサービスとして調達するだけで攻撃を実行できます。攻撃は自動化やサービス化によって大規模にスケールできますが、防御は人材・予算・運用能力に依存するため、攻撃側のような速度では拡充できません。

さらに、AIがこの傾向を加速させています。攻撃者はAIを活用することで、標的企業の調査、フィッシングメールの作成、脆弱性探索、マルウェア開発、侵害後の探索や情報整理といった作業を効率化できます。その結果、従来は高度な知識や多くの時間を必要としていた活動を、より少ない人員とコストで実行できるようになっています。（図1）

図1 AI時代に拡大する攻撃側・防御側の非対称性



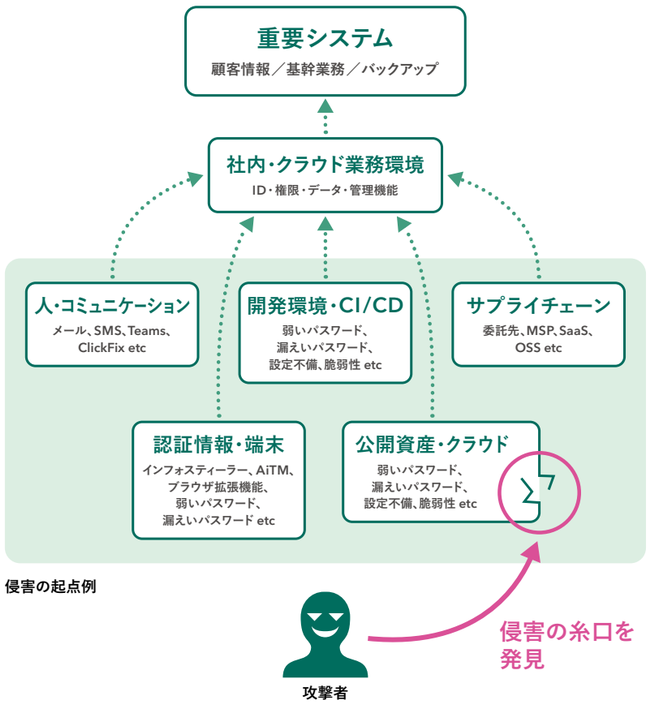
攻撃者はココを狙っている！

攻撃者は侵入にあたり、メール・認証情報・公開資産・委託先など、さまざまな起点を利用します。考慮すべき

は、多くの攻撃者が「重要なシステム」を狙うのではなく、「もっとも侵入しやすい場所」を探している点です。そのため、組織が十分に管理できていない公開サーバ、委託先、利用者アカウントなどが攻撃の糸口として狙われます。

攻撃者に狙われやすい侵入口には、次のようなものがあります。（図2）

図2 攻撃者は重要システムへ正面突破せず、弱い経路から回り込む



●フィッシングメール

現在も主要な侵入口です。生成AIを活用することで自然な日本語のフィッシングメールを大量作成できるようになり、従来よりも見分けがむずかしくなっています。

●SMS・コミュニケーションツール

メール対策が進んだ結果、SMS、Teams、Slackなどのコミュニケーションツールが標的となっています。利用者が日常的に使うチャネルほど警戒心が低下しやすく、攻撃者に悪用されるケースが散見されます。近年は、AIによる音声合成やディープフェイクを利用した〝なりすまし〟も増えています。

●ClickFix によるソーシャルエンジニアリング攻撃

ClickFix（クリックフィックス）は、偽のキャプチャ認証画面やエラー画面を介して、利用者自身に不正なコマンドを実行させるソーシャルエンジニアリング攻撃です。修復手順を装って「Windows + R」「Ctrl + V」「Enter」などの操作を誘導し、クリップボードに格納された不正なコマンドやスクリプトを実行させ、マルウェアに感染させたり、認証情報を窃取します。利用者自身に正規の操作と思わせて不正なコマンドを実行させるため、従来のセキュリティ対策だけでは防ぎにくい点が、ClickFix の特徴です。

●AiTMとデバイスコードフィッシング

近年、パスワードを窃取するだけでなく、認証プロセスや認証後の利用権限を悪用して、正規利用者になりすます攻撃が確認されています。

AiTM[*1]は、偽の認証画面を中継して認証情報やセッション情報を取得します。デバイスコードフィッシング[*2]は、利用者を正規の認証画面へ誘導し、攻撃者が用意した認証要求を承認させることで、アクセストークンなどを取得します。多要素認証を利用しているケースでも、不正アクセスにつながる危険性があります。

例えば、Microsoft 365 の認証済みセッションやアクセストークンが悪用されると、Outlook メール、Teams、OneDrive、SharePoint など複数のサービスにアクセスされる恐れがあります。Microsoft 365 はメールだけでなく、組織の認証・業務基盤として利用されるため、アカウント侵害の影響が広範囲に及ぶ可能性があります。

●侵害されたアカウント

侵害された取引先や委託先のアカウントが攻撃基盤として悪用されることがあります。正規のメールやメールスレッドを利用するため見分けにくく、認証情報の窃取、AiTM、デバイスコードフィッシングに誘導されると、被害が連鎖的に拡大する場合があります。

●ブラウザ拡張機能

ブラウザ拡張機能も新たな侵入口として注目されています。特に近年は、AI関連ツールやPDF編集ツールなど業務効率化ツールを装った悪意のあ

*1 AiTM：Adversary-in-the-Middle（アドバーサリ・イン・ザ・ミドル）の略。利用者と正規のサービスとのあいだに攻撃者が入り込み、認証情報や認証済みのセッション情報を盗み取る攻撃。

*2 デバイスコードフィッシング：スマートテレビや会議用デバイスなどの「デバイスコードフロー」を悪用した攻撃。利用者を正規の認証画面へ誘導し、攻撃者が用意したデバイスコードを入力させることで、攻撃者側の端末にサービスへのアクセスを許可させる。

る拡張機能が確認されています。また、表向きは便利な機能を提供しながら、裏でCookie、認証トークン、閲覧情報を収集したり、後日のアップデートで不正なコードを配布したりするケースもあります。さらには、正規の拡張機能や開発者アカウントが侵害・譲渡され、正規ストアからのアップデートを通じてマルウェアが配布される事例も確認されています。

●VPN・リモートアクセス

VPNやリモートアクセス製品は、侵入に成功すると社内ネットワークへの足掛かりとなるため、継続的に狙われています。公開された脆弱性や漏えいした認証情報を悪用した攻撃は現在も多く発生しており、VPN機器やリモートアクセス基盤は、攻撃者にとって主要な標的の一つとなっています。

インフォスティーラーと攻撃の分業化

近年のサイバー攻撃は高度に分業化されており、攻撃者が一人で全ての工程を担う必要はなくなっています。例えば、インフォスティーラー*3が端末に感染して、認証情報や認証済みセッションを示すCookie、認証トークンなどを窃取し、その情報や侵害済み端末へのアクセス権をInitial Access Broker（IAB）*4が売買します。その後、それらを購入した別の攻撃者が不正アクセスやランサムウェア攻撃を実行するといった流れです。

認証情報やアクセス権は攻撃者コミュニティにおいて売買される商品と化しており、侵害された端末やアカウントそのものが攻撃の足掛かりとして利用されます。そのため、一台の端末感染や一つのアカウント侵害が、情報漏えいやランサムウェア被害など大規模なインシデントに発展する場合があります。

サプライチェーンは近道になる

攻撃者は、重要な組織・システムではなく、もっとも侵入しやすい場所を狙います。委託先、SaaS、OSS、MSP*5、CI／CD*6環境など、周辺組織や関連システムが侵入口となることも少なくありません。本命の組織・システムが堅牢であっても、その周辺が弱点となることは多々あります。

ゼロデイより、Nデイが狙われる

ゼロデイ脆弱性は注目を集めますが実際の侵害では、修正プログラム公開後も未対応の既知脆弱性を狙う、いわゆるNデイ攻撃が多く確認されています。攻撃者にとって、未知の脆弱性を探すより、放置された既知の脆弱性を悪用するほうが効率的なのです。そのため、脆弱性管理やパッチ管理は依然として重要です。

AIは、攻撃者をどう変えるのか

AIは攻撃のライフサイクル全体に影響を与えています。情報収集・フィッシングメール作成・脆弱性探索・マルウェア開発支援・侵害後の探索活動など、攻撃に要する多くの工程が高速化・効率化されています。

AIによって新たな攻撃手法が生まれることも懸念されています。しかし、さらに悩ましいのは、既存の攻撃がより速く、より安く、より大規模に実行可能になっている点です。それと同時に、攻撃の効率が向上し、参入障壁も低下しています。

AIは攻撃側と防御側の双方で活用されていますが、攻撃者の効率化によって、先に指摘した人材・コスト・スケールの非対称性がさらに拡大するのではと危惧されています。

防御側もAI時代へ

防御側でも、脆弱性分析・ログ分析・脅威ハンティング・インシデント対応などへのAI活用が進んでいます。調査や分析の一部をAIで自動化することで、限られた人員でもより多くの脅威に対応できる可能性があります。

しかし、どの資産を守るべきか、どのリスクを許容するかといった判断をAIが代替してくれるわけではないため、AI時代においても、自社のリスクとリソースを踏まえた現実的なリスクベースアプローチは必須です。

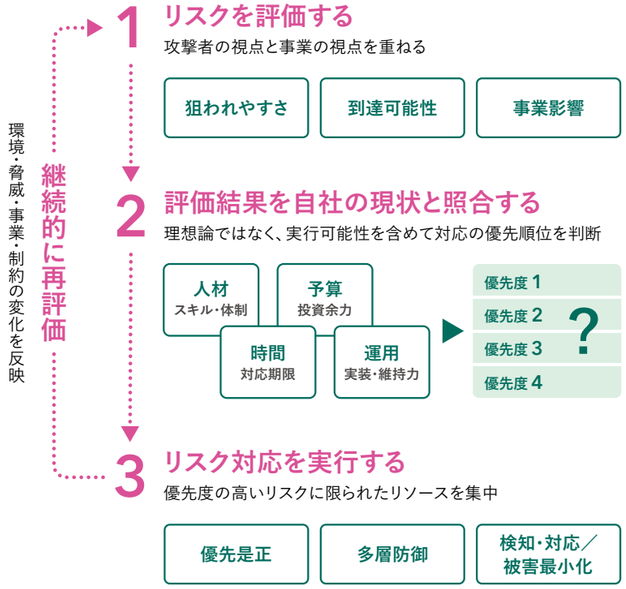
また、AIによって防御の効率は向上しますが、攻撃者と防御側の非対称性は依然として残存しているため、本当に重要な資産・業務を見極めて、限られた防御リソースを優先度の高い領域へ投下することが求められています。（図3）

「外から見える自社」を継続的に確認

防御側が優先順位を判断する際、社内の管理台帳を確認するだけでは十分ではありません。攻撃者と同じ視点で「外部から自社がどのように見えているか」を注視する必要があります。

把握していない公開サーバ、古いドメイン、管理されていないクラウドサービスは、格好の侵入口となる可能性があります。また、採用情報や技術ブログ、SNS、GitHubなどの公開情報

図3 自社の制約を踏まえた現実的なリスクベースアプローチ



を組み合わせることで、利用製品、クラウド構成、開発体制などが推測される場合があります。個々の情報に機密性がなくても、攻撃準備や標的型攻撃に利用される恐れがあるのです。

こうしたことから、公開資産の棚卸、不要なサービスの停止、脆弱性対応、認証情報管理、アクセス権の見直しなどを継続的に行なうことが重要です。特に、把握していない外部公開資産は、監視やパッチ適用の対象から漏れやすく、攻撃者に狙われやすい存在です。

侵入を完全に防ぐ前提を見直す

どのような対策を講じても、侵入を完全にゼロにすることは現実的ではありません。そのため、防御の範疇は「侵入を防ぐこと」から、「侵入されても被害を最小化すること」へと広がっています。侵入後の早期検知、権限拡大や横展開の抑制、重要データへの到達防止、そして迅速な復旧までを含めた対策を考えることが肝要です。

侵害時の影響範囲を限定するには、特権アカウントの分離、不要な権限の削除、ネットワークや環境の分離、重要ログの保全、バックアップからの復旧確認などは欠かすことができません。また、対策を導入するだけでなく、実際に機能する状態が維持されているかを定期的に確認しておくことも大切です。

AIは分析や調査を支援してくれる強力な手段ですが、最終的なリスク判断や経営判断を代替してくれるわけではありません。AIが示したリスクや対応案をそのまま受け入れるのではなく、根拠となるログや資産情報を確認し、事業への影響度を踏まえて、人が判断を下さなければなりません。

AI時代においても、防御の本質は変わりません。侵入を前提に備え、被害を限定し、迅速に復旧できる体制を整えること。そして、自社にとって重要な資産に防御リソースを集中すること。「侵入させない」だけでなく、「侵入されても被害を最小化できる」――これは、AI時代においても変わらないセキュリティの基本です。

AI時代のセキュリティ

攻撃者はターゲットに対し、もっとも侵入しやすい場所を探して、弱い経路から回り込みます。近年、メール・Teams・ClickFix・ブラウザ拡張機能・AiTM・デバイスコードフィッシング・VPN・委託先……等々、侵入口は多様化しています。さらにAIによって、情報収集からフィッシング、侵害後活動まで攻撃のライフサイクル全体が高速化・効率化されています。攻撃者のAI活用にともない、新たな手法の登場だけでなく、攻撃者と防御側の非対称性がさらに拡大していることにも留意すべきです。

今、まさに重要なのは、全てを守ろうとすることではなく、想定されるリスクと本当に守るべき資産を見極め、限られた防御リソースをプライオリティの高い対策に集中することです。「侵入させない」ことに加え、「侵入されても被害を最小化する」ことが、AI時代のセキュリティに求められています。

*3 インフォスティーラー：パソコンなどに感染し、ID・パスワードやCookie、認証トークンなどの情報を盗み出すマルウェア。

*4 Initial Access Broker：企業や組織のネットワークへの侵入口を確保し、認証情報やアクセス権を他の攻撃者に販売するサイバー犯罪者。

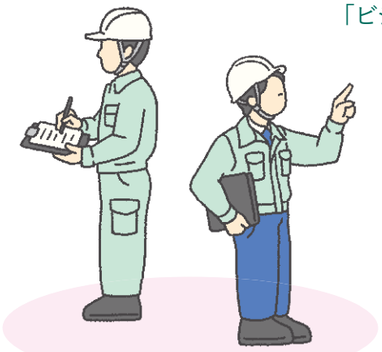
*5 MSP：Managed Service Providerの略。企業に代わって、サーバやネットワークなどのITシステムを継続的に監視・運用・管理する事業者。

*6 CI/CD：Continuous Integration / Continuous Delivery または Continuous Deployment の略。ソフトウェアの変更を継続的に取り込み、ビルド・テストやリリースを自動化する仕組み。

自社の備えを、今一度、確かめてみませんか

自社のセキュリティ対策は、有事の際にも想定通り機能するだろうか？
守るべきはシステムや情報だけでなく、日々の業務、そして顧客や取引先との「信頼」である。
本稿では、ランサムウェア被害などを例に、
「ビジネスを続けるための備え」として見直すべきポイントを整理する。
加えて、自己採点できる「簡易チェックリスト」を用意した。
自社の備えを再確認する一助としてご活用いただきたい。

IIJ ネットワークサービス事業本部
セキュリティ本部 セキュリティビジネス推進部 インテグレーション課長
小宅 洋光



セキュリティ対策の状況を自己点検することは、ビジネスと信頼を守るために必要な取り組みです。現状を把握し、改善を進めることで、サイバー攻撃や情報漏えいによる影響を小さくできます。セキュリティ対策の目的は、単にシステムや情報を守るだけでなく、その先にある日々の業務継続、そして顧客や取引先との「信頼」を守ることにあります。この機会にセキュリティ対策を「ビジネスを続けるための備え」という視点から見直してみませんか。

セキュリティ対策の目的

●「信頼」を守るために

企業のビジネスは、価値を提供し、その対価を得ることで成り立っています。ただし、一度かぎりの商品提供や取引が完了しただけでは、長く事業を続けていくことはできません。顧客に再び選ばれること、取引先との関係が続くこと、従業員が安心して働けること、社会から受け入れられることなどが欠かせません。そして、その土台となるのが「信頼」です。価値と対価によってビジネスは成立し、信頼を積み重ねることが、事業の成長を支えます。

●業務と信頼の両方に影響するサイバー攻撃

現在の企業活動は、受注・生産・販売・顧客対応・請求・決済など、多くの業務がＩＴによって支えられています。そのため、ひとたびサイバー攻撃を受けると、その被害は単にシステムやデータを使えなくなるだけではありません。「商品やサービスを提供できない」、「顧客対応ができない」、「請求や決済ができない」など、さまざまなかたちでビジネスに支障をきたします。

●業務復旧に向けた力

万が一、「情報漏えい」が発生した場合、原因究明、影響範囲の調査、必要に応じた報告、関係各所への通知、顧客や取引先への説明などが求められます。こうした対応力に加え、業務を平常に戻すまでの復元力など、自社の「備え」を一つずつ確かめておきましょう。

公開データから見る実態

例えば「ランサムウェア」に感染した場合、影響は端末だけにとどまりません。業務停止・データの暗号化・調査・復旧・報告や説明に至るまで、影響は広範囲に及びます。

令和八年上半期のランサムウェア被害報告件数は一二三件で、半期ベースでは統計開始以降で最多となりました。その内訳は、中小企業七九件、大企業三一件、団体等一三件でした。中小企業の被害の多さが目につきますが、企業規模を問わず、対策の重要性が高まっています。

感染後に起こり得ることの代表例は、次の通りです。

- 不正アクセスに気づくのが遅れ、被害が拡散した。
- ファイルやシステムが使えなくなり、通常業務が行なえなくなった。
- 非公開の基幹システムにまで影響が及び、甚大なビジネスインパクトを被った。
- さまざまなステークホルダに報告・説明しなければならず、対応にかかるコストが膨大になった。

こういった事態は、結果として売上・取引・信頼を損ない、ビジネスリスクを増幅します。

問題発生時にきちんと機能するか？

ランサムウェア対策では、感染を防ぐだけでなく、早期発見、被害の局所化、重要データの保全、優先度に応じた業務の復旧、関係者への適切な説明など、種々の対応に関する「備え」が不可欠です。

実際に被害を受けた企業・団体を対象とした調査によると、「サイバー攻撃を想定したＢＣＰを策定していた」と回答した企業・団体は、全一一一件のうち二〇件にとどまりました。また、個人情報保護委員会の指導事例では、公表済みの脆弱性の放置、推測されやすいＩＤ・パスワード、アクセス制御の設定ミスなど、安全管理措置の不備が確認されています。

こうした事例からも明らかなように、導入済みの対策が適切に運用され、問題発生時にきちんと機能する状態にあるか、日頃から点検しておくことが重要です。

備えを見直す進め方

皆さんの会社では、これまでに導入してきた対策や「備え」を十分に生かせていますか？「備え・日々の運用・緊急時の対応」を、ワンセットとして定期的に確認し、改善を心がけることが企業を守る力になります。

セキュリティ製品やサービスを導入することは、対策のゴールではありません。大切なのは、導入した対策によって想定されたリスクを減らせているか、問題が起きた時にも予定通り動けるかを普段から確かめておくことです。

備えを見直すためのポイント

①何を守る対策か？

その対策で守るべき重要な業務やシステム、データを洗い出し、導入目的を改めて整理する。

②現在どう使われているか？

設定・運用・監視の状況が、当初の目的に適っているかを確認する。

③問題時にも動けるか？

検知した後の連絡・判断・隔離・復旧までの流れを、手順書や訓練を通じて確かめる。

④不足をどう改善するか？

事業への影響度、緊急性、実現のしやすさを踏まえて、着手する順番を決める。

ここまで述べてきた「自社の備え」を確認できる自己点検のための「簡易チェックリスト」を用意しました。次項を参照しながら、自社のセキュリティの現状を確認してみてください。

参考文献

- 警察庁「令和７年におけるサイバー空間をめぐる脅威の情勢等について」（2026年３月）
  https://www.npa.go.jp/news/release/2026/20260310001.html
- 警察庁「令和８年におけるサイバー空間をめぐる脅威の情勢等について」（2026年９月）
  https://www.npa.go.jp/news/release/2026/20260909001.html
- 個人情報保護委員会「令和８年度第１四半期における漏えい等報告の処理状況」（2026年９月２日）
  https://www.ppc.go.jp/files/pdf/260902quarter-report_roueihoukoku.pdf
- 個人情報保護委員会「令和８年度第１四半期における監視・監督権限の行使状況の概要」（2026年９月２日）
  https://www.ppc.go.jp/files/pdf/260902quarter-report_kengenkoushi.pdf
- IPA「セキュリティマネジメント指導（テーマ別）実施要領 テーマ６セキュリティアセスメント」
  https://www.ipa.go.jp/security/reports/sme/rcu1hd000000kbnh-att/riss_consulting-toolkit_6.pdf

自己点検簡易チェックリスト

「CSF 2.0」*で示された6機能をもとに、自社のセキュリティを確認するための「自己点検簡易チェックリスト」を作成しました。
簡易チェックリストは、IIJ Sketch & Draw Workshopの「セキュリティ対策鮮度チェック」をベースにしています。
IIJ Sketch & Draw Workshop　https://www.iij.ad.jp/workshop/

＊CSF2.0：米国国立標準技術研究所（NIST）が公開している、組織のサイバーセキュリティリスクの管理・低減に役立つ枠組みであり、「Cybersecurity Framework」の略。バージョン「2.0」は以下の6機能で構成されている。

- ❶ 統治（組織としての方針・体制を定め、根づかせる）
- ❷ 識別（何を守るべきかを把握する）
- ❸ 防御（守るための仕組みを整える）
- ❹ 検知（いち早く異常に気づく）
- ❺ 対応（問題発生時に適切に動く）
- ❻ 復旧（業務・データを元に戻す）

1

各項目について、以下の4段階評価で自己点検しましょう。

評価基準　〇…できている　△…一部できている　×…できていない　？…把握していない

※「?」は悪い回答ではなく、確認すべき場所が見つかったサインです。不明な項目は、推測で「〇」にせず、「?」を選び、確認事項として残しましょう。

No.	CSF機能	確認項目	対策分類（参考）	評価
1	統治	セキュリティ方針・ルールを文書化し、関係者に周知している	教育・ルール	
2		従業員向けのセキュリティ教育・標的型メール訓練などを継続的に実施している		
3		サイバーセキュリティ戦略を定期的にレビューしている		
4	識別	自社の重要な業務と、それを支えるシステム・データを整理できている	資産・構成	
5		利用中のPC・スマートデバイスの台数やOSバージョンを把握している		
6		VPN機器・ネットワーク機器の一覧と、管理担当者が明確になっている		
7		クラウドサービス（SaaS／IaaS）の利用状況を一元的に把握している		
8		取引先・委託先と自社の、ビジネス上・システム上の関係を把握している		
9	防御	管理者アカウントと一般アカウントを分離し、必要最小限の原則にもとづいて運用している	ID・権限	
10		重要システムや外部接続に多要素認証を導入している		
11		退職・異動の際、アカウント・権限を速やかに変更・削除している		
12		特権アカウントの利用状況を記録し、定期的に確認している		
13		OS・ソフトウェアのセキュリティ更新を計画的に適用している	脆弱性・更新	
14		外部からアクセス可能なIT資産の脆弱性を定期的に診断・調査している		
15		システムを構成するソフトウェアの部品構成（いわゆるSBOM）を把握し、脆弱性情報を確認・対応する担当者および手順が決まっている		
16	防御	サポート終了製品を把握し、更新・入れ替えの計画を立てている	脆弱性・更新	
17		業務利用端末にマルウェア対策ソフト（EPP／EDRなど）を導入している	感染・データ喪失	
18	検知	ファイアウォール・VPN・認証・重要システムのログを取得・保存している	異常検知	
19		不審な通信、ログイン失敗、権限変更などを検知・通知できる仕組みがある		
20		影響範囲や原因を調査可能なかたちで、ログを確認・分析できる		
21		夜間・休日を含めた監視・連絡方法を決めている		
22		端末の不審な挙動を検知し、対応できる運用体制がある	感染・データ喪失	
23	対応	インシデント発生時の連絡フロー、判断者、社内外の役割分担が明確になっている	初動・連絡体制	
24		インシデント発生時に、対応の備えが機能する状態にある（外部支援の要否を含む）		
25		情報漏えいなどが発生した際、報告・本人通知の要否を確認する手順がある		
26		過去1年以内に、机上訓練または実動訓練を行なっている		
27		感染を想定した初動対応の手順が決まっている	感染・データ喪失	
28		感染した端末・アカウントを速やかに隔離・停止できる		
29	復旧	重要なデータのバックアップを、復旧対象と接続されていない環境に保管している	感染・データ喪失	
30		バックアップから重要業務を復旧する訓練を実施している		

2

1のチェック結果を「セキュリティ対策全体像」で確認しましょう。

① 機能ごとに〇・△・×・？を数えると、「どこが対策できていて、どこに見直しの余地があるか」を全体像として把握できます。

②「〇」の数で全体の状態を見たあとに、「×」「？」の内容を確認します。

※右記は本記事用の簡易な目安であり、認証・監査・第三者評価を意味するものではありません。

※「〇」の合計が25個以上でも、いずれかの機能（特に項目数の少ない「統治」「復旧」など）に「×」や「?」が集中している場合、総合判定によらず、その機能を最優先でご確認ください。

No.	CSF機能	〇	△	×	?
1–3	統治	個	個	個	個
4–8	識別	個	個	個	個
9–17	防御	個	個	個	個
18–22	検知	個	個	個	個
23–28	対応	個	個	個	個
29–30	復旧	個	個	個	個
	合計	個	個	個	個

判定条件	目安	確認・行動
〇が25個以上	「備え」の実効性を確認	現状の運用を継続し、定期的な見直しと訓練で有効性を確かめます。
〇が17～24個	「備え」の見直し・強化を検討	△・×・？を機能別に整理し、重要業務への影響が大きいものから改善します。
〇が16個以下	何から「備え」が必要かを整理	対策の全体像と優先順位を整理し、体制・運用・技術の不足を段階的に補います。

3

チェック結果から、必要な対策を考えましょう。

不足している備えと業務への影響を整理し、対策・サービスの種類を検討します。
「×」「？」が付いても、すぐに製品を追加すればいいとは限りません。
何が不足しているか、どの業務に影響するか、既存の対策を十分に生かせているかを確認してから、必要な対策の種類を整理します。

No.	CSF機能	点検で見えた課題	検討したい対策	サービスの種類
1–3	統治	教育・ルールを見直したい	セキュリティ教育、標的型メール訓練、規程策定、運用改善支援	●IIJセキュリティ診断ソリューション 標的型メール攻撃訓練 ●IIJセキュリティコンサルティング ●IIJセキュリティドクター
4–8	識別	資産・構成がわからない	IT資産管理、構成管理、ネットワーク・クラウド利用の可視化	●IIJ統合運用管理サービス ●IIJセキュアエンドポイントサービス ●IIJ CASBソリューション
9–17	防御	ID・権限管理、更新・脆弱性対応、端末のマルウェア対策に課題	統合ID管理、多要素認証、特権ID管理、アクセス制御、脆弱性診断、脆弱性管理、更新管理、EPP／EDRなどマルウェア対策	●IIJ IDガバナンス管理サービス ●IIJ IDサービス ●IIJ脆弱性管理ソリューション ●IIJセキュアエンドポイントサービス ●IIJ統合運用管理サービス ●IIJフレックスモビリティサービス／ZTNA ●IIJ脆弱性診断ソリューション ●IIJアタックサーフェスアセスメントソリューション
18–22	検知	異常に気づけない	ログ管理、SIEM、SOC、MDR、端末監視（EDR）などの監視・分析サービス	●IIJ C-SOCサービス ●IIJデータ可視化ソリューション ●IIJマネージドファイアウォールサービス ●IIJマネージドIPS／IDSサービス
23–28	対応	初動・連絡体制、インシデント発生時の対応に不安	緊急対応支援、調査支援、対応手順策定、机上訓練、端末・アカウント隔離支援	●IIJ C-SOCサービス ●IIJ CSIRT構築／運営アドバイザリソリューション ●IIJセキュリティドクター ●IIJデジタルフォレンジック調査 ●IIJセキュリティ教習所
29–30	復旧	バックアップからの復旧に備えたい	隔離バックアップ、復旧支援、復旧訓練	●IIJシンプルバックアップサービス ●IIJセキュアエンドポイントサービス ●IIJセキュリティドクター

IIJ Research
となりの情シス

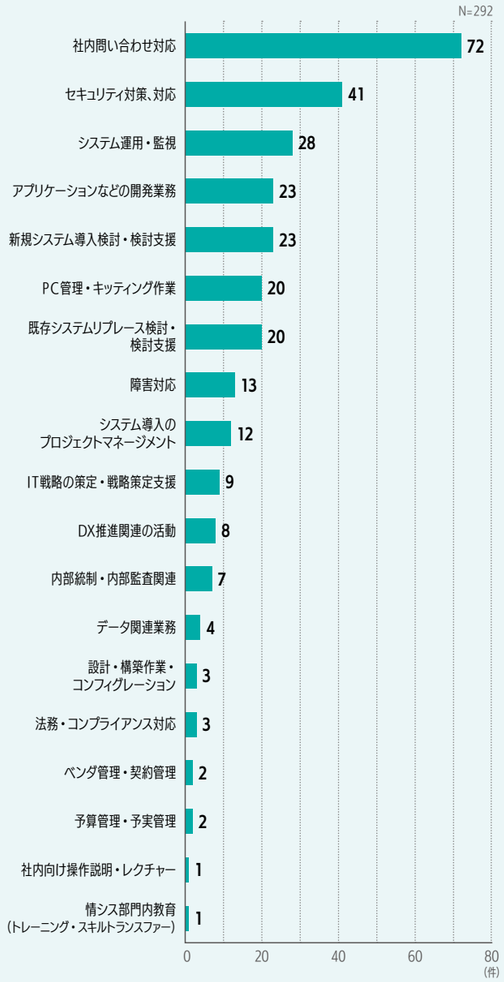
情シスの「ホンネ」と「リアル」がわかる！

全国情シス実態調査2026

2021年から実施している「全国情シス実態調査」を2026年も実施。
今回は定番の設問に加え、導入したITツールの効果についても調査しました。

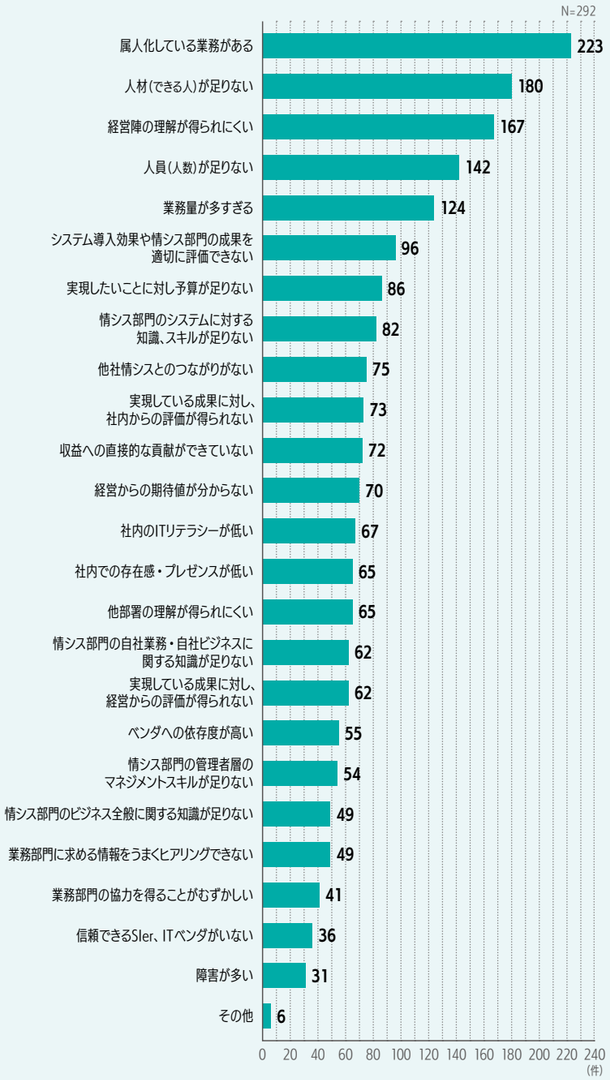
（実施期間：2026年6月4日～10日／有効回答数：292件）

Q1. もっとも時間を費やしている日々の業務を教えてください。



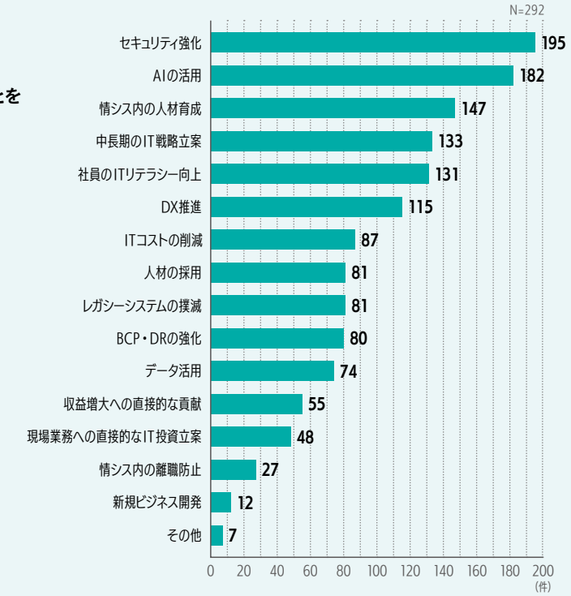
- 2年連続第1位だった「既存システムリプレース検討・検討支援」は第6位となり、昨年、第2位だった「社内問い合わせ対応」が第1位に。昨年まで第9位だった「アプリケーションなどの開発業務」は第4位にランクインした。
- 役職別に見ると、管理職層においても、日々の定常業務の負荷が一定量あり、本来注力すべき戦略・企画機能への時間シフトが十分に進んでいない特徴が明らかになった。

Q2. 貴社の「情報システム部門」の課題を教えてください。（複数回答可）



- 情報システム部門の課題のトップは「業務の属人化」。従業員規模を問わず、もっとも多く挙げられた。
- 「人材不足」「人員不足」など、質と量の両面で人材に関する課題が上位を占めた。

Q3. 情報システム部門として、今後「強化すべき／したい」ことを教えてください。（複数回答可）

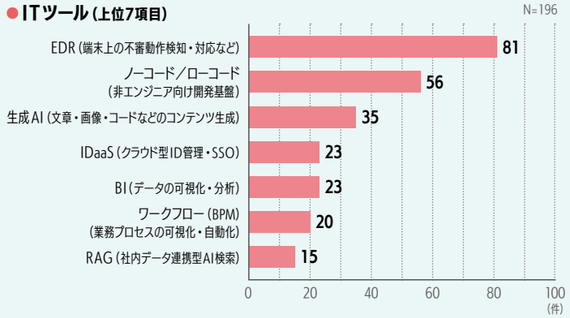


- 第1位は「セキュリティ強化」、第2位は「AIの活用」となった。
- 「情シス内の人材育成」は、従業員数100人未満の企業では第5位に留まる一方、それ以外では、いずれも上位に位置しており、企業規模が大きくなるほど関心が高まる傾向が見られた。

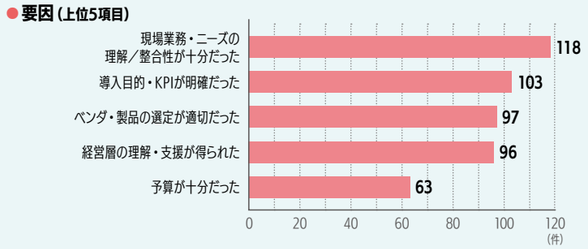
Q4. 過去3年に導入したITツールのうち、効果が高かった／低かったものと、その要因を教えてください。

効果が高かった

●ITツール（上位7項目）

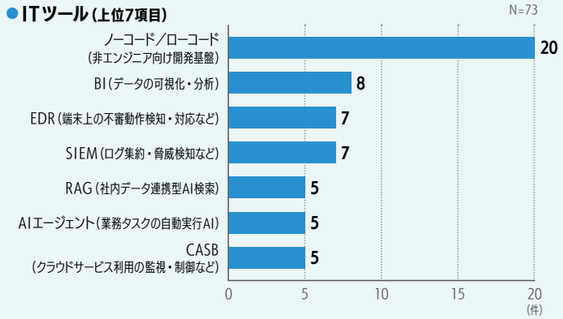


●要因（上位5項目）

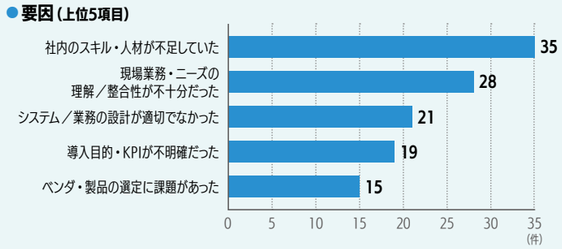


効果が低かった

●ITツール（上位7項目）



●要因（上位5項目）



- 効果が高かったツールは「EDR」「ノーコード／ローコード」「生成AI」の順。成功要因の第1位は「現場業務・ニーズの理解／整合性が十分だった」で、導入成果を左右する鍵は「現場理解」にあることがうかがえた。
- 一方、効果が低かったツールでも「ノーコード／ローコード」が最多。要因の第1位は「社内のスキル・人材が不足していた」で、「現場ニーズとの整合性の不足」が続いた。

今年で6回目となる「全国情シス実態調査 2026」のアンケート調査結果をお届けしました。特設サイト「法人IT調査レポート」では、本稿で取り上げた項目以外にも、今後、強化・習得したいスキルや情シスのお悩みなど、情シス部門のリアルな声を紹介しています。ぜひこちらもご覧ください。

IIJ 情シス BOOST UP PROJECT のご紹介

「IIJ 情シス Boost-up Project」は、情報システム関連部門で働く皆さまに日々の活動や組織運営のヒントとなる情報をお届けしています。

HP
https://www.iij.ad.jp/svcsol/jboost/

X
@IIJ_Jboost

人と空気とインターネット

自分の目で見て、手で触れながら考える

IIJ 非常勤顧問
株式会社パロンゴ監査役、その他 ICT 関連企業のアドバイザー等を兼務
浅羽 登志也

州街道、甲州街道という五街道の起点でした。ここから日本各地へ人や物が旅立ち、また全国から人や物や文化が集まってくる。始まりの場所であり、同時に帰着する場所でもありました。だからこそ、重要な場所を守るために、阿形と吽形の一対が置かれているのでしょう。

しかも麒麟という存在自体が面白い。龍に似た頭、鹿のような胴体など、複数の動物の特徴をあわせ持つ想像上の聖獣です。その龍もまた、鹿の角、蛇のような胴、魚の鱗、鷹の爪など、多くの動物の特徴を内包しています。獅子像にも、狛犬や西洋のライオン像など、複数のモチーフが混ざっているようです。一つの姿のなかに、多くのものが折り重なった聖獣たち。そのうえ、それらが阿吽の一対となり、日本中へ道が広がる起点・終点に立っているわけです。

さらに現在の東京は、世界中へ人や物事を送り出し、同時に世界中から人や物事が集まる世界都市です。すると日本橋の麒麟像は、まるで現在の東京の姿を百年以上前から象徴し、また守ってきたもののようにも見えてきます。よく見るとこの麒麟像にはさらに翼がついています。もしかすると、「これからの東京、あるいは日本という国は、外へ開かれ、さまざまなものを受け入れながら発展する場所でありたい」という未来への意思まで込められていたのではないか。そこまで考えるのは、考えすぎでしょうか？　こんなふうに立ち止まって眺めていると、何気なく通り過ぎていた橋の欄干が、急にいろいろなことを語り始めてくれます。

昨今なら、こうしたこともまず生成ＡＩに聞けば、考えるまでもなく教えてくれるでしょう。「この像は何か」「麒麟とはどんな動物か」「日本橋はどんな場所か」……尋ねれば、ほんの数秒で詳しい説明が返ってきて、とても便利です。

でも、ここで少し引っかかります。もし最初からＡＩに聞いていたら、ＡＩなりに一通りの説明を詳しくしてくれたかもしれません。でも、そのとき筆者は、麒麟像の口の形に自分で気づき、反対側へも回って確かめて、日本橋の歴史と阿吽の意味を自分なりに結びつけて考えたでしょうか？　たとえ詳しい説明をしてくれたとしても、筆者は深く考えることなく「ふーん」と表面的な理解で終わっていたのではないかと思います。すぐにＡＩに答えを教えてもらうことによって、逆に、そこに込められた大事なメッセージを読み落としてしまうこともあるのかもしれません。

日本橋で考えたこと

先日、日本橋を歩いて渡っていたときに面白いことを発見しました。橋の中央に一対の麒麟像があります。よく見ると二頭の口の形が違う。「これも阿吽なのか？」と思って反対側へ回ってみると、そちらもやはり阿吽の一対でした。さらに橋の入口と出口には、阿形・吽形の獅子像まで置かれています。どうして寺社仏閣でもない日本橋に、こんなものが置かれているのでしょうか？

日本橋は江戸時代、東海道、中山道、日光街道、奥州街道、甲州街道という五街道の起点でした。ここから日本各地へ人や物が旅立ち、また全国から人や物や文化が集まってくる。始まりの場所であり、同時に帰着する場所でもありました。だからこそ、重要な場所を守るために、阿形と吽形の一対が置かれているのでしょう。

しかも麒麟という存在自体が面白い。龍に似た頭、鹿のような胴体など、複数の動物の特徴をあわせ持つ想像上の聖獣です。その龍もまた、鹿の角、蛇のような胴、魚の鱗、鷹の爪など、多くの動物の特徴を内包しています。獅子像にも、狛犬や西洋のライオン像など、複数のモチーフが混ざっているようです。一つの姿のなかに、多くのものが折り重なった聖獣たち。そのうえ、それらが阿吽の一対となり、日本中へ道が広がる起点・終点に立っているわけです。

さらに現在の東京は、世界中へ人や物事を送り出し、同時に世界中から人や物事が集まる世界都市です。すると日本橋の麒麟像は、まるで現在の東京の姿を百年以上前から象徴し、また守ってきたもののようにも見えてきます。よく見るとこの麒麟像にはさらに翼がついています。もしかすると、「これからの東京、あるいは日本という国は、外へ開かれ、さまざまなものを受け入れながら発展する場所でありたい」という未来への意思まで込められていたのではないか。そこまで考えるのは、考えすぎでしょうか？　こんなふうに立ち止まって眺めていると、何気なく通り過ぎていた橋の欄干が、急にいろいろなことを語り始めてくれます。

昨今なら、こうしたこともまず生成ＡＩに聞けば、考えるまでもなく教えてくれるでしょう。「この像は何か」「麒麟とはどんな動物か」「日本橋はどんな場所か」……尋ねれば、ほんの数秒で詳しい説明が返ってきて、とても便利です。

でも、ここで少し引っかかります。もし最初からＡＩに聞いていたら、ＡＩなりに一通りの説明を詳しくしてくれたかもしれません。でも、そのとき筆者は、麒麟像の口の形に自分で気づき、反対側へも回って確かめて、日本橋の歴史と阿吽の意味を自分なりに結びつけて考えたでしょうか？　たとえ詳しい説明をしてくれたとしても、筆者は深く考えることなく「ふーん」と表面的な理解で終わっていたのではないかと思います。すぐにＡＩに答えを教えてもらうことによって、逆に、そこに込められた大事なメッセージを読み落としてしまうこともあるのかもしれません。

ＡＩの言うことを鵜呑みにしない

生成ＡＩは、わからないことを、あっという間に「わかったこと」に変えてくれます。しかし、人間にとって本当に大切なのは、すぐに答えを知ることではなく、なんとなく違和感を持つこと、わからないまま眺めること、そこから自分なりに意味を見つけていくこと――そのプロセスにこそ、大切な働きがあるのではないでしょうか。

そう考えると、最近読んでいる仏教の話につながってきました。仏教では、人間が世界を認識する仕組みを、六根、六境、六識という言葉で説明します。眼、耳、鼻、舌、身、意が六根。それに対応する、色や形、音、香り、味、触感、そして思考の対象となるのが六境。さらに、六根が六境に触れることで六識、つまり認識が生まれるとされています。私たちは、世界そのものを直接認識しているわけではなく、世界にある何かに自分の感覚が触れ、それを自分の側で構成する。

その結果として、自分にとっての「世界」が立ち現れてくるわけです。そして、その先に快・不快という感覚が生まれます。快であれば、もっと欲しいし、不快であれば、遠ざけたい。そのようにして欲望や嫌悪や執着、いわゆる〝煩悩〟が生まれてくるのです。

生成ＡＩは私たちと世界とのあいだに入って、見たいものをもっと見せ、知りたいことをよりわかりやすくし、自分の考えに沿った説明まで返してくれます。これは便利である反面、かなり危ういことにも思えます。生成ＡＩは、人間の煩悩を満たす装置であるだけでなく、煩悩そのものを増幅する装置にもなり得るからです。

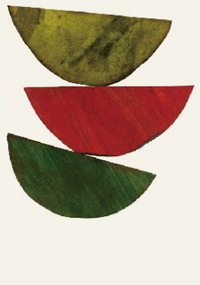
ＡＩは、私たちの考えに対し、筋の通った答えを返してくる傾向があります。すると「やはり自分の考えは正しかった」と思いやすくなる。でも、それは本当に世界を直視していることになるのでしょうか？

ここで、仏教が説く「無明（むみょう）」という言葉を思い出します。自分では世界を正しく見ていると思っているけれど、実はそうではない。ＡＩが心地よい世界をつくってくれればくれるほど、私たちは「無明」になっていくのではないか。もし生成ＡＩが、人間の煩悩増幅装置にもなり得るとすれば、ＡＩの言うことを鵜呑みにせず、自分の頭で考えながら世界と向き合い、どう関係を結ぶかが大事なのでしょう。

パソコンに向かってばかりでなく、時々街に出かけて、いろいろなものを自分の目で見て、手で触れながら考えることも必要だなと、日本橋を渡りながら感じました。

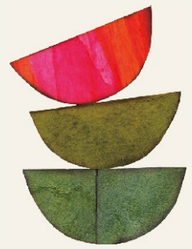
阿から始まり、吽で終わる。その一連の思考のプロセスを自分の中でしっかりと踏まえることが大切なのだ――そんなことを寺院の入口に安置された一対の仁王像が語っていたのかもしれません。





AIに聞けば数秒で答えが出る昨今、
私たちは世界を直視しているだろうか？
今回は、自らの感覚を働かせ、
迷いながらも考える“プロセス”の意義を考察する。





イラスト／末房志野

Technical Now

教育・研究を支える情報基盤をリプレース

―― Microsoft Azureとオンプレミスを組み合わせ、用途に応じた最適なシステム基盤を構築

創価大学の学内システムのリプレースにあたり、一部サーバのクラウド化、ネットワークの最適化、より安定的な情報基盤の構築などをIIJが担当。リプレースから運用に至る一気通貫のサポート体制が高い評価と信頼を獲得した。

[導入前の課題]
ブラックボックス化したネットワークの可視化と、構成・コストの最適化

―― 皆さまの所属とシステムリプレースにおける役割を教えてください。

細田　私たちの課は管理職を含む9名で、開発チームと運用チームに分かれています。開発チームは学生向けポータルサイトなどを内製し、運用チームはネットワーク、セキュリティ、サーバ環境などインフラ全般を担当しています。

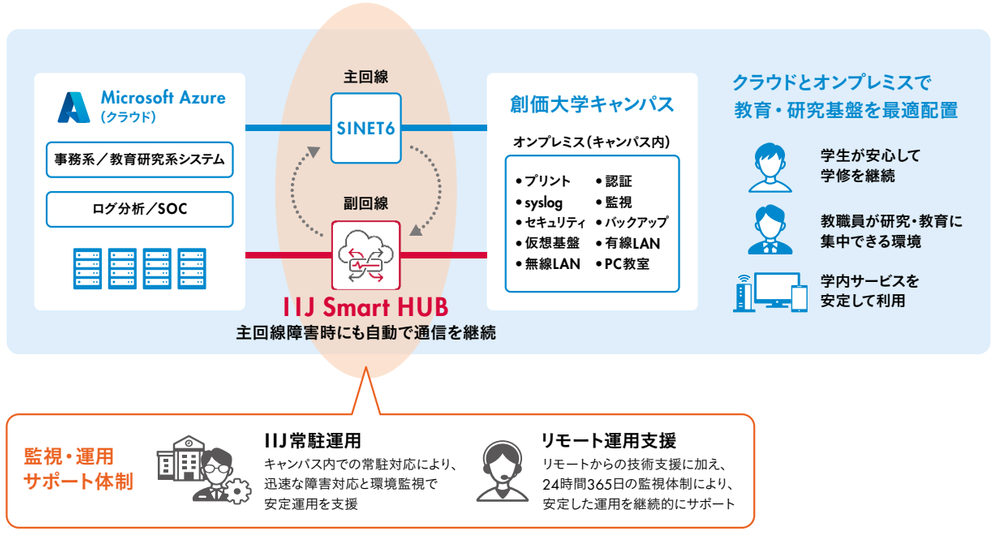
―― ネットワークインフラに関してどのような課題をお持ちでしたか？

本多　本学は学内システムを5年周期でリプレースしていますが、ネットワークインフラは長年、単一ベンダに運用・管理を任せていました。大学側の担当者が交代してもベンダは変わらなかったため、細かな設定のナレッジなどはベンダ側にしか蓄積されておらず、大学側は把握していない、いわゆる「ブラックボックス化」した状態でした。加えて、構成自体を見直す時期でもあったことから、次のリプレースではネットワークに強みを持つベンダを選びたいと考えていました。

細田　利用している機器が本学に合っているのか、コストが適正なのかという懸念もありました。また、認証もMicrosoftの認証基盤と大学独自のID認証などがいくつも組み合わさって複雑化していたため、今回のリプレースを機に統合したいと思っていました。

―― IIJとの接点はどのように生まれたのですか？

本多　IIJさんとはインターネット回線サービスを通じて以前からお付き合いがありました。今回、RFP（提案依頼書）に対して最初に提示された構成案が非常に具体的で、クラウド基盤へ移行したあとの構成まで明確に示されていて、私たちの状況や要望を深く理解していただいたことに驚きました。



※ 本記事は2026年7月に取材した内容をもとに構成しています。記事内のデータ、組織名、役職などは取材時のものです。

[選定の決め手]
課題を踏まえた具体的な提案 一気通貫のサポート体制

―― IIJを評価された点を教えてください。

細田　本学が提示した要件は「セキュリティの担保」、「学生のBYOD（Bring Your Own Device）への対応」、「クラウド活用」、「コスト適正化」の4つです。同じメーカの機器を長年使い続けるなかで価格が上昇していたうえに、本学の実情に対してオーバースペックな構成ではないかとも考えていました。

最終的に5社の提案書とプレゼンテーションの内容を比較検討しました。そのなかで、私たちの課題をもっとも具体的に理解し、全体最適な提案に落とし込んでくれたのがIIJさんでした。特に、ネットワークの可視化という課題への理解、機器構成の見直しによるコスト適正化の提案、さらには、ネットワークだけでなく、サーバや認証システム、セキュリティなども、リプレースから運用まで一気通貫で支援していただける点を高く評価しました。

―― 機器を大きく変えることに不安もあったのでは？

本多　長年利用し安定稼働していた機器を変えることには不安もありましたが、IIJさんには提案していただいた機器を他大学へ導入した実績があり、その大学の方ともお話しできる機会を設けてくださったので、不安は軽減されました。構成や機器の変更にともなうネットワークのポリシーやルールの見直しもフォローしていただき、大変助かりました。

―― Microsoft Azureとオンプレミスのハイブリッド構成は、どのように設計・移行されたのですか？

細田　本学では早い段階からクラウド活用を進める方針がありましたが、負荷の大きいサービスはオンプレミスに残す必要があったため、Microsoft Azureとオンプレミスを組み合わせたハイブリッド構成を採用しました。

クラウドへの移行にあたっては、約200台の仮想サーバについて、どのシステムをオンプレミスに残して、どれをクラウドに移せばいいのかという点も精査してくださいました。

本多　実際の移行では、中央教育棟と本部棟にあるサーバルームが光回線などでつながっており、パッチケーブルの接続状況を細かく把握しきれていなかったのですが、IIJさんが前のベンダの資料を参照しながら丁寧に確認してくださり、私たち自身もネットワークの状況を理解できました。その結果、数日間にわたる切り替え作業も大きなトラブルなく完了しました。

[導入後の効果]
冗長化と24時間365日の監視体制 より安定した情報基盤を構築

―― ネットワーク刷新後の効果をどう感じていますか？

細田　大きな効果を感じているのが、ネットワークの冗長化です。従来からマルチホーム構成でしたが、副回線の帯域不足が課題でした。メイン回線のSINETは、一度、障害が発生して副回線に切り替わった際、帯域が足りず、授業や業務に支障が出たことがありました。そこで今回、副回線を増速し、障害時にも安定した通信を維持できる帯域を確保しました。Microsoft Azureへの接続も冗長化したので、SINETの障害で副回線へ切り替わった場合でも、クラウド上のサーバを継続利用できます。

―― 現在、IIJのサポートをどのように活用されていますか？

細田　IIJさんにはネットワークだけでなく、サーバや認証、セキュリティを含む教育研究システム全体について、構築後も支援していただいています。現在、IIJさんのエンジニアが本学に常駐し、常駐メンバーだけでは対応がむずかしい案件は、リモートのSEが技術面からサポートしてくれます。

小松　いつも迅速に対応してくださり、内容によっては、依頼当日のうちに対応を完了していただけます。PCの入れ替え時にも設定作業などをお願いでき、負担が大きく軽減されました。

小林　運用を担うメンバーがそれまでとは別のチームになりましたが、運用開始後も大きなトラブルはなく、教職員や学生の問い合わせにもスムーズに対応してくださっています。

―― セキュリティ面ではどのような変化がありましたか？

本多　監視の仕組みを丁寧に作っていただき、24時間365日の監視体制が整いました。以前は大量のアラートを確認しきれないこともありましたが、現在は対応すべきアラートが絞り込まれ、優先順位に沿って対処できるようになりました。

―― 今後の展望や、IIJへの期待をお聞かせください。

細田　事務系のPC環境のリプレースを予定しているので、IIJさんにはゼロトラストをはじめ、さまざまな知見の共有や提案を期待しています。

本多　クラウド基盤の活用を教員の研究分野にも広げていきたいと考えています。従来、研究用サーバの利用には機器の調達や設置が必要で、利用開始までの負担が大きかったのですが、今回構築した基盤の一部を研究用途に活用できれば、教員の研究活動への支援につながります。また、今後は避けて通れないAIを含む発展的なIT活用もIIJさんに相談しながら進めていきたいです。

創価大学

創価大学（https://www.soka.ac.jp/）
大学キャンパス：〒192-8577 東京都八王子市丹木町1-236
開学：1971年4月2日
学生数：約6000名（学部生・大学院生／2026年5月1日現在）
専任教員数：334名（教授・准教授・講師・助教／2026年5月1日現在）

1971年に東京都八王子市で開学した総合大学。建学精神に「人間教育の最高学府たれ」「新しき大文化建設の揺籃たれ」「人類の平和を守るフォートレス（要塞）たれ」を掲げて、教育・研究を展開。現在、7学部10学科・6研究科・2専門職大学院を設置している。

創価大学 総合学習支援オフィス システム支援課

課長	副課長	副課長	係長
細田 隆志 氏	本多 光紀 氏	小松 光昭 氏	小林 師 氏



導入したサービス・ソリューション

- IIJ GIO with Microsoft Azure
- IIJ GIO with Microsoft Azure / ExpressRoute
- IIJ Smart HUB
- インテグレーションサービス

Information インフォメーション

1 データ活用の目的を整理する無償ワークショップを開始

IIJは、法人向けに2022年から実施している無償ワークショップ「IIJ Sketch & Draw Workshop」の新プログラムとして、「データ利活用目的整理ワークショップ」の提供を開始しました。データの可視化・分析の仕組みづくりに着手する前に、「何のデータを使うのか」「誰が何を知りたいのか」「なぜ可視化・分析するのか」を整理します。IIJがファシリテーターとして議論の進行と意見の言語化を支援し、業務部門とシステム部門の合意形成を後押しすることで、その後の要件定義やシステム構築へ円滑に進める状態を目指します。

● **ワークショップの流れ**　全3回（各回2時間）を約2カ月にわたって実施します。

Day 0	事前ガイダンス	ワークショップの概要・目的、全体スケジュールの共有、宿題説明
Day 1	目的・現状の整理	現状の課題の共有、目的の整理
Day 2	画面・システムの整理	どう見るか、システム・データの整理
Day 3	イメージの確認・意見交換	可視化イメージの共有・意見交換

アウトプット
- 要件定義ワークシート
- 載せるべき情報の一覧
- システム・データの一覧
- 可視化のイメージ

● **参加費用**　無料
● **詳細**　https://www.iij.ad.jp/workshop/

2 IIJ 2026 TECHアドベントカレンダー

IIJのエンジニアが技術的な情報や取り組みを発信している公式ブログ「IIJ Engineers Blog」では、毎年12月に「アドベントカレンダー」を開催しています。アドベントカレンダーとは、クリスマスまでの日々を1日ずつ数えて楽しむカレンダーのこと。これになぞらえて、12月1日から24日まで、IIJグループの社員が日替わりで記事を執筆・公開します。日々の業務で得た知見や、技術への探究心から生まれたテーマなど、さまざまな技術に関するコンテンツが並びます。年末のひととき、エンジニアたちの多彩な記事をお楽しみください。



● **開催日**　2026年12月1日～24日
● **詳細**　https://eng-blog.iij.ad.jp/adventcalendar2026/（12月1日から公開予定）

Internet Trivia インターネット・トリビア

脆弱性アップデートはなぜ「予告」されるのか？



IIJ 広報部 技術統括部長
堂前 清隆

サイバーセキュリティに関する大きな話題が立て続けに発生しています。情報漏えいなどの事故を防ぐには、システムの「脆弱性」を解消していくことが重要です。オープンソースソフトウェアなど、外部から導入したソフトウェアの場合、各ソフトウェア開発者からアップデートやパッチが公開されるため、これを自分が管理しているシステムに適用して、その脆弱性に対処します。

重大な脆弱性の場合、アップデート公開前に日時を指定した「予告」が行なわれることがあります。問題が見つかればすぐにアップデートを公開すればいいのにと思われるかもしれませんが、そうもいかない事情があります。

開発者視点で、脆弱性対応で避けなければならないことは何か？ それは、アップデートが十分に行き渡らないあいだに、その脆弱性を使った攻撃が蔓延することです。アップデートが公開されると、前のバージョンとの差分から、脆弱性の詳細や攻撃の手がかりがわかってしまい、攻撃者に悪用されることがあります。詳細が広く知られていなかった脆弱性の場合、アップデートが公開されることで攻撃リスクが高まるのです。

そうしたリスクを最小限にするために、システム管理者がスムーズにアップデートを適用できるようにする準備が、限られた関係者によって行なわれます。サーバで使われるソフトウェアは、開発者が提供したものをそのまま利用するだけではありません。Linuxディストリビューション向けに「パッケージ化」されたものや、Dockerなどを利用して「コンテナ化」されて使われることもあります。ソフトウェアによっては、オリジナルの開発者がパッケージやコンテナの管理者と連携して、一般公開前のソフトウェアを提供し、あらかじめパッケージのアップデートを準備してもらうこともあります。

こうした準備を整えたうえでアップデートの公開に至るわけですが、いくらパッケージやコンテナが揃っていても、突然、公開されたアップデート情報を各システムの管理者がキャッチアップするのはむずかしいため、準備の進捗状況をにらみながら公開の日時を決め、脆弱性のアウトラインとともに発表し、システムの管理者に準備を促すのです。

システム管理者も、ただ予告された日を待つわけではありません。サーバで稼働しているソフトウェアは、他のソフトウェアと組み合わせて動かすことがほとんどです。脆弱性対応のアップデートであっても、ソフトウェアの変更には違いなく、これまで問題なく動いていた組み合わせがアップデートによって正しく動作しなくなることもあります。この組み合わせはシステムごとに異なりますし、場合によっては自社開発のソフトウェアが含まれているかもしれません。ですので、アップデート後にシステムが正しく動作するかは、システムごとに確認する必要があり、その確認には人手と時間もかかります。アップデートが公開されたのち、早急に確認を済ませる必要があるので、人員の手配や作業手順の確認なども行なわれます。

このように脆弱性対策が進められるのは一つの理想ですが、残念ながらうまくいかないこともあります。準備の途中で情報が外部に伝わってしまうケースもあり、そのような時は、攻撃のリスクが高まったとして、予定を前倒しして急きょアップデートが公開されることもあります。

日常生活や仕事においてシステムは欠かせなくなっており、脆弱性への迅速な対応はますます重要になっています。現場のエンジニアは、気の休まらない日々が続きます。

株式会社 インターネットイニシアティブ

本社	東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム 〒102-0071	TEL：03-5205-4466
関西支社	大阪府大阪市中央区北浜 4-1-1 淀屋橋ゲートタワー 18F 〒541-0041	TEL：06-7638-1400
名古屋支社	愛知県名古屋市中村区名駅南 1-24-30 名古屋三井ビルディング本館 4F 〒450-0003	TEL：052-589-5011
九州支社	福岡県福岡市博多区冷泉町 2-1 博多祇園 M-SQUARE 〒812-0039	TEL：092-263-8080
北海道支店	北海道札幌市中央区北二条西 4-1 札幌三井 JP ビルディング 18F 〒060-0002	TEL：011-218-3311
東北支店	宮城県仙台市青葉区中央 4-4-19 アーバンネット仙台中央ビル 11F 〒980-0021	TEL：022-216-5650
横浜支店	神奈川県横浜市港北区新横浜 2-15-10 YS 新横浜ビル 8F 〒222-0033	
北信越支店	富山県富山市牛島新町 5-5 タワー 111 5F 〒930-0856	TEL：076-443-2605
中四国支店	広島県広島市南区松原町 2-62 広島 JP ビルディング 16F 〒732-0822	TEL：082-568-2080
沖縄支店	沖縄県那覇市久茂地 1-7-1 琉球リース総合ビル 2F 〒900-0015	TEL：098-941-0033
新潟営業所	新潟県新潟市中央区東大通 1-3-1 INPEX 新潟ビルディング 4F 〒950-0087	TEL：025-244-8060
豊田営業所	愛知県豊田市西町 4-25-13 フジカケ鐵鋼ビル 5F 〒471-0025	TEL：0565-36-4985

IIJ グループ／連結子会社

株式会社 IIJ エンジニアリング
東京都千代田区神田須田町 1-23-1 住友不動産神田ビル 2 号館 15F 〒101-0041 TEL：03-5205-4000

株式会社 IIJ グローバルソリューションズ
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム 〒102-0071 TEL：03-6777-5700

ネットチャート株式会社
神奈川県横浜市港北区新横浜 2-15-10 YS 新横浜ビル 〒222-0033 TEL：045-476-1411

株式会社 IIJ プロテック
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム 〒102-0071 TEL：03-5205-6766

株式会社センシフィア
東京都新宿区東五軒町 6-22 フロントプレイス飯田橋 〒162-0813 TEL：03-5205-6890

株式会社トラストネットワークス
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム 〒102-0071 TEL：03-5205-6490

IIJ America Inc.
55 East 59th Street, Suite 18C, New York, NY 10022, USA TEL：+1-212-440-8080

IIJ Europe Limited
1st Floor 80 Cheapside London EC2V 6EE, U.K. TEL：+44-0-20-7072-2700

IIJ Global Solutions Singapore Pte. Ltd.
160 Paya Lebar Road #03-07 Orion @ Paya Lebar Singapore 409022 TEL：+65-6773-6903

PTC SYSTEM (S) PTE LTD
10 Kallang Avenue #07-12 Aperia Singapore 339510 TEL：+65-6282-0255

艾杰（上海）通信技術有限公司
邮编 200031 上海市徐匯区長楽路 989 号 世紀商貿広場 3 階 301B-302 TEL：+86-21-8026-1899

この冊子の内容はサービス形態・価格など予告なしに変更することがあります。（2026年11月作成）
※ 表示価格には、消費税は含まれておりません。
※ 記載されている企業名あるいは製品名は、一般に各社の登録商標または商標です。
※ 本書は著作権法上の保護を受けています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。
©Internet Initiative Japan Inc. All rights reserved. IIJ-MKTG001-0197

発行／株式会社インターネットイニシアティブ 広報部
お問い合わせ／株式会社インターネットイニシアティブ 広報部内「IIJ.news」編集室
〒102-0071 東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム TEL：03-5205-6310 E-mail：iijnews-info@iij.ad.jp

編集／村田茉莉、増田倫子、笹島貴明、中島優
編集協力／合同会社 Passacaglia
表紙イラスト／末房志野
デザイン／榊原健祐、榊原吏海（Iroha Design）
印刷／株式会社興陽館 印刷事業部

コラム vol.14

パラフェンシング 笹島貴明の Allez!（アレ）

IIJ 広報部 笹島 貴明

アジアパラ競技大会で二つの銅メダルを獲得！

名古屋で開催されたアジアパラ競技大会が閉幕しました。アジアパラとしては初の日本開催となる記念すべき大会で、筆者はフルーレ団体とエペ団体で銅メダルを獲得しました！ 大会の二週間前からイラク代表チームと合同合宿を国内で実施し、大会期間中はパーソナルコーチやトレーナーも帯同するなど、普段の大会とは異なる万全の環境で試合に臨むことができました。また、会場に足を運んでくれた家族、友人、日頃から応援してくださっている皆さん、さらには、現地の小学生からの応援が大きな力になり、メダル獲得の推進力となりました。本当にありがとうございました！

筆者は二〇一八年にインドネシアで開催されたアジアパラに参加し、普段の大会とはまったく異なる充実した待遇とともに、過密な日程、そして人生初めての国際大会でのメダル獲得が非常に印象深いのですが、名古屋開催の本大会も食堂や宿泊施設などの設備、各種イベントがとても充実していました。試合日程は六日連続かつ合計七種目という超過密スケジュールで疲労との戦いになりましたが、最後まで怪我することもなく大会を終えることができました。

筆者は力を入れてきたエペという種目の個人戦のメダル獲得を第一目標としていたのですが、ベスト16で中国選手に勝利したのち、続く準々決勝で中国の別の有力選手に10-15で負けてしまいました。ロサンゼルス・パラリンピックの選考という点から、個人の戦績を重視していただけに非常に悔しいのですが、今まで背中も見えなかった中国選手に勝利の道筋が見えたのは大きな収穫でした。今後の大会でリベンジを果たして、パラリンピック出場を勝ち取ります！

今大会で一番うれしかったのは、四日目に開催されたエペ男子団体のメダル獲得です。二日目に獲得したフルーレ団体の銅メダルもうれしかったですが、エペ団体はこれまでアジアパラでメダルを獲得した経験がなく、前日のエペ個人戦での悔しさをぶつけたいと思って挑んだ種目でした。銅メダルをかけた三位決定戦のウズベキスタン戦は、選手のリレー方式の最終戦で29-29のどちらかが1点とれば勝利！ という大接戦になり、最後はアンカーの安直樹選手が1点をもぎ取って勝利するという劇的な結末になりました。この試合は一生の思い出になりそうです。

このように非常に充実した大会になりましたが、目標としていた個人戦でのメダル獲得には一歩届かず、ロサンゼルス・パラリンピック出場に向けて、さらに練習していく必要性を改めて感じました。引き続き応援よろしくお願いいたします！



事前合宿のイラクの Ali Ammar 選手との練習の様子。左が筆者。

表紙の言葉

パリのモンマルトルで、お目当てのパン屋を探しながら石畳の小道を歩き回りました。初めて歩く私には迷路のような道も、そこで暮らす人にはいつもの通り道。ふと足元に目を向けると、一つひとつ表情の異なる四角い石が敷き詰められていました。

末房志野



IIJ.news はWebでもご覧いただけます。
バックナンバーも公開しています。
URL：https://www.iij.ad.jp/iijnews/

編集後記

いまだに今年が令和何年か、すぐに出てきません。先日も「令和7年」と書かれた予定表が出てきて、今年のものか去年のものかわからず、夫に「今年って令和何年だっけ?」と聞くと、すぐに「8年」と返ってきました。即答できるのが不思議で聞いてみたところ、「西暦の下2桁を足した数が令和の年になる」と教えてくれました。もっと早く知りたかったです。（M）

学生時代、大学に「青島（チンタオ）レコード」という演劇サークルがあり、大好きでよく公演を観に行っていました。主宰・岡田望さんの脚本が本当に面白く、解散後もどこかで書いていないかと、ときどき名前を検索していたほど。当時の看板俳優は、今や『VIVANT』『田鎖ブラザーズ』などで大活躍の山中崇さん。先日、山中さんがゲストのトーク番組を観ていたら、なんと岡田さんが登場！ 今は児童書の編集者をされているそう。当時の台本や写真とともに、何年検索してもわからなかった岡田さんの「今」が、思いがけずテレビから届いて、嬉しくなりました。（T）

先日、親戚の紹介で国立競技場のVIP席ともいえる Prime Ground というところでJリーグを観戦しました。コース料理のような食事がついたり、おいしいお酒を楽しめるラウンジもすごかったのですが、コーナーキック横のピッチサイドで観戦するサッカーは大迫力！ ピッチレベルの視点は、正直なところ、何が起こっているのかTV観戦よりもわかりにくいのですが、ライブ感というべき独特の楽しさがありました。（S）

年の瀬が近づくと、「またね」「いってらっしゃい」と手を振る機会が増えてきます。そもそも、なぜ手を振るのでしょう。このしぐさは、「魂振り（たまふり）」という古い習わしの名残ともいわれています。昔の人は別れ際に袖を振り、相手の無事を願ったそうです。何気なく振る手にも、相手を思う気持ちが込められているのですね。それでは皆さま、また来年。（Y）



IIJ

Internet Initiative Japan