KPMG Newsletter

KPMG Insight

特集 サイバーセキュリティ対策を通した事業成長の在り方

Vol. 63

November 2023

「サイバーセキュリティが事業成長を後押しする」グループをまとめ上げるソフトバンクのガバナンス体制

DXによる生産性向上、IoTによる社会生活の利便性向上など、あらゆるシーンで通信の重要性が増すなか、ソフトバンクはライフラインの一端を担う通信事業者として、社会全体のセキュリティ向上に努めています。有事の際にも通信を止めずデータを守るために、サイバーセキュリティをさらに強く安全なものにするために、日頃どのような対策に取り組んでいるのか。人材育成やシステムの構成管理における工夫は何か。今回は、ソフトバンク株式会社 常務執行役員 CISO（最高情報セキュリティ責任者）兼 サイバーセキュリティ本部 本部長の飯田 唯史 氏にお話を伺いました。

【インタビュアー】

KPMGコンサルティング
執行役員パートナー
澤田 智輝

所属・役職は、2023年9月時点のものです。

インシデント対応の肝は、初動対応における人間同士のコミュニケーション

澤田　ソフトバンクには事業領域が異なるグループ会社がたくさんありますが、全部で何社くらいあるのでしょうか。

飯田　2023年8月現在、約300社近くのグループ会社があり、その業種や業態は多岐にわたります。各社の事業内容や提供サービス、ビジネス環境は絶えず変化と進化を続けており、私たちはグループ会社と継続的なコミュニケーションを取りながら、各社の事業動向を注視し、新たなセキュリティ上のリスクや課題がないかを常に見きわめています。

澤田　グループのセキュリティをリードする責任者として、有事に備えていつも心がけていることがあれば教えてください。

飯田　グループ会社でセキュリティインシデントが発生した場合、情報収集を含む初動が重要となります。大規模地震などの自然災害の発生時と同様に、セキュリティインシデントも発生直後は、何が起こったのか分からず混乱やパニックが起こりやすいです。この混乱が続くと、被害が広がって深刻化し、財務的な損失を招く可能性もあります。したがって、発生直後こそ素早く状況を把握し、的確な対策へ結びつけセキュリティ上のリスクの低減・お客様への影響を限定的にし、経済的な影響を最小化することを心がけています。

澤田　初動で必要な情報を集めるために、最も重視することは何でしょうか。

飯田　一言でいえば、インシデント発生部門の人たちとの密なコミュニケーションを確立することです。ソフトバンクでは、これまでさまざまな規模、種類のインシデントを経験してきました。これらの経験を通じて、社内ではインシデント発生時に必要なコミュニケーションパスが迅速に確立できるようになっていますが、グループ会社でインシデントが発生したときは少し状況が違います。グループ会社といっても我々とは別の会社ということもあり、会社間を跨いだ情報連携が遅れる場合が時々発生します。また、グループ会社側もインシデントの初動対応でバタバタしていますから、我々としても待っているだけでは必要な情報をタイムリーに入手できません。その意味で初動対応時のコミュニケーションパスの確立が一番大切で、一番困難なポイントといえます。この課題を克服するため、我々が積極的にグループ会社側と会話しながら、被害内容や影響範囲などを把握し、取るべき暫定対応や恒久対策をグループ会社と伴走しながら確認・確立していきます。

また、有事の際に限らず、平時においてもグループ会社のセキュリティ責任者や担当者とは密に情報連携し、コミュニケーションパスを確立・維持するよう心がけています。その際の課題としては、セキュリティの人材不足が挙げられます。実際いくつかのグループ会社においては、人材不足を理由にやむを得ずセキュリティに精通していない人材をセキュリティ責任者や担当者にアサインしている会社もあるため、我々のセキュリティ人材をグループ会社に兼務・出向させるなどして人的サポートも行っています。また、異動や退職などに伴ってセキュリティ責任者や担当者の入れ替わりも発生します。そうなると責任者や担当者との関係をイチから構築しなおす必要がありますが、異動や退職はどの会社にも共通して発生しますので、それらを前提にしたグループ会社との関係構築、維持強化を心がけています。

澤田　これまでさまざまなインシデントを経験されてきたと思いますが、飯田さんはいつもどのような心構えで対応しているのでしょうか。

飯田　職責上、セキュリティインシデントを発生させないという覚悟をもって職務に就いていますが、それでもインシデントは発生します。ただし、我々はインシデントが発生しても「転んでもタダでは起きない」という心構えで常に対応します。弊社では「一度経験したインシデントは二度と起こさない」ために徹底した再発防止策を講じるという企業風土があり、結果としてセキュリティレベルはどんどん向上していきます。実際、平時においては「そこまでする必要があるのか？」と言われるほど強度が高い（＝副作用を伴う）セキュリティ対策も、インシデント発生を通じて社内での合意形成を経て講じてきた対策事例はいくつもあります。また、インシデント対応を通じて「同じ釜の飯を食った仲間」という感覚が芽生え、社員間の絆がグッと深まります。仮に将来、別のインシデントが発生したとしても、以前に比べて格段にスムーズな連携、タイムリーな対応が可能になります。インシデントを経験してどんどんレジリエンスが高まっていると実感しています。

澤田　転んだ時にしっかりと、徹底的に学ぶということですね。

飯田　はい。「何がいけなかったのか？」「どうすべきだったのか？」を学ぶことが大事ですね。インシデント対応時だけでなく、机上訓練や実地訓練においても、毎回、反省材料や改善ポイントが必ず出てきます。完璧な対応ができた、反省材料がない、改善ポイントが見つからない、といったケースはまずないですね。

「セキュリティハザードマップ」で、各社のシステム構成を可視化する

澤田　グループ会社が多種多様な事業を営んでいると、グループでのセキュリティ強化は難しいのではないでしょうか。

飯田　はい、1社1社で事業内容やビジネスモデルが違いますし、システムの構成も1つとして同じものはありません。そこで、

グループ各社には「セキュリティハザードマップ」というシステムやネットワークの構成を表した図を作成してもらっています。

このマップによって、1）我々およびグループ会社の双方がグループ会社のシステムに関する「土地勘」を高めることができます。また、2）「どこが侵害されると、どういう被害があるのか」「どういう影響が出て、どのような対応が必要になるのか」をグループ会社と共に事前に把握することが可能になります。

さらに、3）グループ会社でインシデントが発生した際、このマップを使って発生箇所などの把握ができ、我々の対応サポートの精度や速度が向上します。

澤田　ハザードマップについて、私はホテルなどに掲示されている避難経路図をイメージしました。消防隊が駆け付けた際に各階の構造が一目で分かるのと同じですね。システムやネットワークの構成がわかっていないと、飯田さんのチームにインシデントの連絡が来た時にすぐに対処できないですよね。だから、グループ会社にも事前に作っておいてほしいということなのでしょうか。

飯田　そのとおりです。ハザードマップはシステムやネットワークの構成全体をビジュアル化しています。システムはここにあって、ネットワークはこうつながっていて、どんな情報がどこに格納されているか。そういったことをできるだけ可視化するようにしています。ちなみに、グループ会社にはハザードマップの作成をお願いしているものの、ソフトバンクが自社のハザードマップを作るとなると実はかなり大変なのです。

澤田　それはどうしてでしょうか。

飯田　端的に言うと、弊社のITや商用通信のインフラ、各種のサービス提供を実現するプラットフォームなど、それらを構成するシステムやネットワークの数が膨大で、ハザードマップでは表現できないほど複雑だからです。さらに、システムやネットワークの新規追加、統廃合などによる変化は常にありますので、ハザードマップを最新の状態に保ち続けるには多くの労力と時間を要します。ただし、弊社でハザードマップに相当するものがないかといえば、そういうわけではありません。1枚に集約されていないというだけで個々のシステムやネットワークの構成図は存在します。

澤田　まさに地図と似ていますね。地図にも全体地図と詳細地図がありますが、ソフトバンクの場合、詳細地図は完成していて、これから全体地図を整備するという感じでしょうか。

飯田　そうですね。大きな一枚の全体地図が整備され、常に最新の状態に保たれていることが理想ですが、弊社の場合、詳細地図があることでスムーズなインシデント対応が可能です。その意味では、詳細地図の内容を遅滞なくアップデートする重要性がますます高まってきているといえます。

澤田　現場がしっかりと必要な対応を理解できることが大事だと思います。それが把握できるようなレベルでマップを作っているということでしょうか。

飯田　そのとおりなのですが、たとえば個々のシステムやネットワークに内在する脆弱性などは、詳細地図だけでは把握が困難なこともあります。たとえば、米国国立標準技術研究所（NIST）の脆弱性データベース（NVD）などが報告する脆弱性情報は年間2万件を優に超えます。膨大な数のシステムやネットワークを抱える弊社が、システムごとに脆弱性の有無をすべて手作業で確認するのはもはや不可能です。そのため弊社では各システムに潜む脆弱性の特定とパッチ適応など対応の迅速化を目指し、各システムの詳細な構成要素を記録した構成管理データベースを構築・運用しています。加えて、SBOM（ソフトウエア部品表）と呼ばれるソフトウエア管理手法の導入も検討していますが、ライブラリやフレームワークなどの中身までの詳細レベルまで把握できないケースもあり、カバーできる範囲には限界があります。その課題を補うために、インシデント発生を前提とした対応能力（ヒューマンスキル）の向上を図る一方で、対応業務自体の効率化、省力化にも着手し、全体的なレジリエンスのレベルアップを目指しています。

澤田　そういう意味では、インシデント管理は本当に総力戦になるわけですね。今は情報を自動で集めることができますが、そうした情報だけでは解決は難しいのでしょうか。

飯田　そうですね。弊社でもML（機械学習）やRPA（ロボティック・プロセス・オートメーション）を駆使し、脅威情報などのセキュリティ関連情報の自動収集やSOC（セキュリティオペレーションセンター）での監視業務の自動化を進めていますが、まだ道半ばですね。業務の自動化比率はこれから徐々に高めていきますが、完全自動化の実現には程遠く、現在のところまだまだヒューマンオペレーションに頼る部分が多いのが実態です。

セキュリティを機械任せにせず、必ず人間が総合的な判断を

澤田　グループ会社の管理という観点ではどうでしょうか。グループ内には大小さまざまな会社が存在していますが、彼らのセキュリティ全部をマニュアル化するのはなかなか難しそうです。自動化したりAIを使うことになるかと思いますが、オペレーションを効率化するためにどのような取組みをされていますか。

飯田　グループ会社の管理については、OSINT（オープンソース・インテリジェンス）を活用したリスク評価、脆弱性診断サービスの提供、サービスデスクなどを使った情報連携や密なコミュニケーションなど、

Tadashi Iida

飯田 唯史 氏

ソフトバンク株式会社 常務執行役員 CISO（最高情報セキュリティ責任者）兼 サイバーセキュリティ本部 本部長
通信業界におけるキャリアは30年以上。ソフトバンクに2002年入社。以降、通信インフラの設備投資および運用におけるバジェットコントローラーとして通信エリアの拡大や品質改善をサポート。2015年米 Sprint Corporation（現 T-Mobile US）に出向し同社のネットワーク品質改善に従事。2016年にソフトバンクに帰任後、モバイル通信インフラの企画部門および西日本エリアのネットワーク構築部門を歴任。2018年より最高情報セキュリティ責任者（現職）。

ITを駆使したさまざまな取組みを進める一方で、セキュリティ人材のグループ会社への兼務や出向、セキュリティ監査などの地道な施策も多数あります。

グループ会社のセキュリティに関するクオリティコントロールを実施するうえで、マニュアル化は有効な手段の1つだと思うのですが、マニュアルにしたがってセキュリティ対策を講じられる人材や能力がその会社に備わっていなければ絵に描いた餅です。その意味でセキュリティ人材の不足は深刻な課題だとあらためて認識させられます。

またAI活用や自動化は人材不足を補う手段としてだけでなく、これまで人が担っていた業務を自動化することで、業務全体の効率化や生産性の向上に大きく貢献すると期待しています。

澤田　人がやってみてはじめて、AIや自動化ツールを入れることの有用性がわかるのかもしれません。何も手をつけていないところにいきなり投資してくださいと言っても、経営からすると「なぜ？」という話になりますから。

飯田　そのとおりだと思います。たとえば、弊社ではSOCで検知するアラートの分析業務の自動化を進めていますが、自動化の業務範囲を闇雲に拡大すれば、誤検知の発生頻度が高まり、却って人の手を煩わせることになります。ですので、人の経験や知見を自動化プロセスにフィードバックして分析業務の精度を高めるようにしています。

澤田　さまざまなセキュリティ製品を使われているかと思いますが、それはグループで統一されているのでしょうか。統一していない場合、統一される予定はありますか？

飯田　セキュリティ製品についてグループ会社からも「親会社が使っている製品を使わないといけませんか？」という問い合わせをもらいますが、答えは「ノー」です。どの製品を使っても構わないと考えています。ただし、我々のSOCでグループ会社のセキュリティ監視をするケースにおいては、我々が使っているセキュリティ製品の利用をグループ会社にお願いしています。理由は単純で、我々が精通しているセキュリティ製品だと監視効率が良いからです。我々も監視に関わる人的リソースは限られていますから、同じカテゴリーのセキュリティ製品なら取り扱う種類はできる限り絞っていきたいと思います。

澤田　今後、セキュリティのシェアードサービスのようなものが、グループ会社の経営では大事になってくるのではないかと考えています。人事や経理ではすでに導入されていますが、セキュリティでも同じようにグループで統合することで効率化できそうな気がします。

飯田　はい、セキュリティ製品はグループ内で統一するのが理想です。共同購買による調達コストの削減も期待できます。しかしながらグループ各社ですでに個別導入しているセキュリティ製品をキャンセルさせ、我々が選定したセキュリティ製品に入れ替えていくにはグループ会社側で相当な手間、時間、コストを要します。加えて、現ベンダーとの契約面の制約があったり、グループ会社が現在利用しているセキュリティ製品の満足度が高く、別製品に入れ替えることに難色を示すケースもあります。こういった事情から、すべてのセキュリティ製品を統一するには数年単位の時間を要すると覚悟しています。

セキュリティ担当者を支援するための取組み

澤田　セキュリティ人材の育成や従業員に対するセキュリティ教育、あるいはセキュリティマインドの醸成については、どのような取組みをされているのでしょうか。

飯田　まず教育に関しては、弊社が自前でさまざまなコンテンツを作成し、社内イントラでいつでも自己学習できる環境を整えています。全社員に向けて定期的にeラーニングなどでのオンライン研修を実施しています。加えてワークショップや模擬訓練などの実地研修も適宜実施しています。これらはグループ各社のセキュリ

ティ教育にも活用できるよう、無償もしくは安価に提供しています。

澤田　今、人材が不足し、セキュリティ人材の確保は難しくなっています。グループ会社のセキュリティ人材やCISOを支援する計画などはありますか。

飯田　我々とグループ会社のセキュリティの責任者・担当者を支援する取組みの一環として、悩み相談や情報の連携・共有などができるような場を設定しています。ただ残念なことに、そうした場があってもセキュリティ感度が低い会社からの積極的な参加は期待できません。ですので、そのような会社に関心をもってもらう取組みも進めています。その一例として、おおよそ2ヵ月ごとに100社以上のグループ会社のCxOが集う会議が開催されます。その会議にて、参加企業すべてを対象に我々が事前に調査・分析したセキュリティヘルスチェックの結果を参加企業単位で発表したことがあります。チェック結果が芳しくなかった会社の幹部は当初バツの悪そうな顔をしていましたが、チェック結果とそれがもたらす潜在リスクを理解いただき、改善活動に着手いただくよう各社のセキュリティ責任者と担当者に早々にご指示いただきました。以降、ヘルスチェックは年間通じて複数回行い、結果を発表する度にグループ会社のCxOには高い緊張感と関心を持って聴講いただき、結果としてグループ会社のセキュリティ感度の底上げに大きく寄与することができたと思います。

澤田　情報開示することで、経営とセキュリティ担当者のコミュニケーションを密にするという役割もありそうです。

飯田　そうですね。その後、低評価だったグループ会社のセキュリティ担当者から直接ご連絡をいただいたこともあります。「なんでダメなのですか？」「どこが悪いのですか？」と根掘り葉掘り聞かれました。なかには、「リスクを針小棒大に評価していないか？」などと反論いただいたケースもありました。セキュリティ担当者は自社の経営層に説明責任があるので理論武装しておきたかったのだと思います。情報開示によって上記のような問い合せ対応に追われましたが、結果としてグループ会社において経営層とセキュリティ担当者間のコミュニケーションの頻度が増えたのは事実のようです。

澤田　親会社のOBを活用して、グループ会社のCISOやセキュリティ担当者を支援するというお話もうかがいました。それはどのような計画なのでしょうか。

飯田　弊社ではマネジメント層の人材に対する役職定年制度があり、既定の年齢（役職レベルに応じて50歳、55歳、57歳）に達すると組織長からのステップダウンを余儀なくされます。役職定年を迎えた役職者は、緊張感が切れ仕事が緩慢になってしまう傾向があります。

澤田　若手にも仕事を任せていかないといけないですし。

飯田　はい。そこで役職定年を迎えたセキュリティ人材を再トレーニングし、グループ会社のCISOとして頑張ってもらおうと考えています。

澤田　再トレーニングとはどういう内容でしょうか。セキュリティのスペシャリストの方に、マネジメントスキルに関する教育を提供するなどでしょうか。

飯田　再トレーニングでは、対象者に「CISOに求められるものは何か？」を理解、習得、実践できるようにサポートしていく予定です。

CISOはセキュリティプロフェッショナルと比較し、戦略マインド、探求心、粘り力、コミュニケーション力、組織を巻き込む力など要求されるレベルが格段に高いです。

もちろんセキュリティプロフェッショナルとしてこれまで培ってきた技術、たとえば、サイバー攻撃の分析および対応、フォレンジックなどはさらに磨きをかけ、後進育成のために技術継承をしていただきたいと思います。

澤田　セキュリティの知識も、社会人経験もある。そういう方がCISOとしてグループ会社の補助をするというのは、グループ会社としても心強いですね。

飯田　はい。しかも彼らはもともと我々のチームメンバーですから、当然ながら我々とのパイプは強固です。我々とグループ会社間の情報連携もし易くなり、インシデントが発生した時にも迅速なサポートが可能です。メリットしかありません。

澤田　グループ会社でインシデントが発生しても、すぐに連携できて親会社を頼れるというのは、いいですね。

飯田　また、我々としては、すでに強固なセキュリティ対応体制やガバナンスを持つ上場企業クラスのグループ会社よりも、むしろ小規模なグループ会社ほど丁寧にサポートする必要があると考えています。小規模なグループ会社でもセキュリティインシデントが発生すると「ソフトバンク系の○○でセキュリティ事故発生」などという見出しで報道につながってしまいますので、CISOの派遣はまずは小規模なグループ会社を対象にしていきます。

セキュリティは事業に寄り添い、成長を後押しするものであるべき

澤田　最後に、グループ会社のセキュリティガバナンスを強化していこうと考えているCISOの皆さんへの応援メッセージをお願いします。

飯田　「セキュリティに完璧はない」とい

われていますが、インターネットを含む外部ネットワークからの遮断や隔離、物理的なアクセス禁止など、極端な施策を講じれば理屈上は実現可能です。しかしながら現代のビジネス環境や現場では事実上不可能だというのは想像に難くなく、だからこそ「完璧なセキュリティは存在しない」という結論に達します。

次のアプローチとして、セキュリティと事業成長の双方が妥協するクロスオーバーポイントを模索していくことが自然の流れになりますが、セキュリティ制御が強すぎると、企業が革新的な技術や新たなサービスを提供するなどのイノベーションを促進しようとする際のブレーキになりかねない。一方、サイバー攻撃は年々高度化し、企業にとっての大きなリスクファクターになってきている。このような議論を繰り返しても、事業成長とセキュリティの対立構造は一向に解消されません。

我々が目指すべきは「事業成長を加速させるセキュリティ」です。事業成長とセキュリティは相反する関係にあるように思えるかもしれませんが、実際のところ、セキュリティは事業成長を加速させる上で重要な役割を担っていると思いますし、それを継続しなければいけないと思っています。

ところで、「ミニ四駆」のレースをご覧になったことはありますか？ネットにも動画がアップされているので、ぜひ一度ご覧になっていただきたいのですが、各車がサイドウォールで仕切られた各トラックを猛烈な速度で疾走している姿はとても迫力のある光景です。このミニ四駆のレースをつぶさに見ているといくつかの発見があります。まず、各車とサイドウォールの間には絶妙なスペースが確保され、各車の動きを過度に制限しないように工夫されている。そして、ミニ四駆側にもサイドウォール接触時の摩擦を軽減する仕組みを導入しておりきわめてスムーズにコースを周回していく。それによって各車は「安心して」全速力でコースを駆け抜けることに集中できる。

そこで、ミニ四駆が事業、サイドウォールがセキュリティと置き換えてイメージしてみてください。事業の推進や成長を高速で実現するには、セキュリティというサイドウォールが必要不可欠です。「各車とサイドウォールの間のスペースの確保」はデバイスを監視しながら認証・認可をする「ゼロトラスト」に通じるものを感じます。また、「サイドウォール接触時の摩擦を軽減する仕組み」はシステムの設計段階から事業側でセキュリティ対策を考慮し組込んでいく「セキュリティ・バイ・デザイン」につながります。実際の事業においては、ミニ四駆レースのようにループ状のコースをグルグルと周回するのではなく、未知な領域に向かって終わることのないコースを突き進んでいかなければなりません。そのためにセキュリティ部門が事業部門に先んじて、新たな脅威や攻撃に対する情報感度を高め、事業部門との密接な連携をとりながら適切なサイドウォールをどれだけ迅速に構築できるかが、セキュリティ部門に求められていることだと思っています。

かく言う我々もまだまだ道半ばであり、偉そうなことを言える立場ではありませんので、弊社では3年前からさまざまな業種の企業のセキュリティ責任者様をお招きし、お互いのベストプラクティスを共有し学び合いながら、セキュリティ対策の強化・改善に努めています。この対談をご覧のセキュリティ責任者の方々とも情報交換や連携ができ、日本におけるセキュリティのレベルアップに少しでも貢献できれば望外の喜びです。

澤田　以前いただいた飯田さんの言葉を借りるなら、「セキュリティはブレーキではなく、ガードレールだ」ということを示していくということですね。本日はありがとうございました。

KPMGコンサルティング株式会社
執行役員パートナー
澤田 智輝(写真左)

セキュリティコンサルタントとして20年以上の経験を有し、海外のKPMGと連携をしたグローバル／グループ全体でのセキュリティ高度化を多数支援。サイバーセキュリティブループリントの策定などの戦略領域からゼロトラストアーキテクチャの実装などのテクノロジー領域まで幅広く支援実績を有する。

KPMGジャパン
home.kpmg/jp