サイバー攻撃防御における情報共有の価値

熱海 徹[†]

現在は「サイバー攻撃者が圧倒的有利」と言われています。セキュリティ脅威に関する情報やインテリジェンスを事業者同士で活用して攻撃の成功を阻止することが、リスクの低減につながると思っています。仮に、事業者ごとに攻撃を仕掛けられたタイミングが異なっても、ある事業者で検知した攻撃やその手法に関する情報をいち早く分析、共有して他の事業者の対策に活用できれば、被害抑止につなげられるのです。今後、進めていくセキュリティについて解説します。

キーワード：サイバー攻撃、セキュリティ対策、リスクマップ、サイバーインシデント、ISAC

1. まえがき

サイバー攻撃を実施しようとする者や攻撃手法の開発は、残念ながら今後も収まることはないと思います。攻撃手法そのものの把握や対応に加え、攻撃者がなぜ攻撃を行うのか、「攻撃の意図」を可能な限り把握することが重要になってきます。そのためには所轄官庁をはじめ、さまざまなセキュリティ機関、類似のセキュリティリスクを抱える組織などと攻撃そのものだけでなくつかんだ予兆などさまざまな情報を交換できる仕組み作りが重要になってきます。情報が相互に交換できる組織やグループはすでに国内に存在していますが、そのほとんどは個人対個人で築いた信頼感をベースとしたものです。この信頼感をどのように組織対組織に広げていけるかが今後のサイバー攻撃への対応における最重要課題と考えます。

2. 攻撃手法の特徴

最近の攻撃手法の中には、企業や組織が利用するサードパーティーのアプリケーションや、取引関係にある特定のウェブサイトなどを悪用して、攻撃者が侵入を試みる「サプライチェーン型」攻撃やウェブサイトなどを悪用する「水飲み場型」攻撃などがあり、ますます巧妙な手口になっています。

特徴は、セキュリティが脆弱な組織を踏み台にする傾向が強いと言えます。

サプライチェーン型に関しては、攻撃者が標的を絞り込んで侵入するための戦術を組み立てやすいと言われており、狙われる側は、正規の取引先やツール、ソフトウェアが攻撃者の侵入口となってしまうため、その特定や防止が

非常に困難です。

また、従来よりメールによるウィルス感染がありますが、近年「ビジネスメール詐欺」など、昨年から、まったく異常なメールとして認識することができない巧妙な手法で金銭目当てに攻撃して来るものが現れてきました。

セキュリティ対策としては「怪しいメールは開封しない」という働きかけをしてきましたが、怪しいと思われないメールを異常と見極めるのは非常に難しいため、改めて多段階の承認プロセスの採用や、メール以外での複数の連絡手段による確認が必要になってきました。

3. インシデントをもたらすヒューマンエラー 4つのNGポイント

私は、長年ヒューマンエラーに起因する放送人為事故の撲滅に取組み、以前在籍した地方局では10年間の無事故を達成することができました。そこで学んだヒューマンエラー、または事例がセキュリティインシデントを引き起こすパターンと共通していることに気がつきました。企業内のセキュリティインシデントにはさまざまな種類がありますが、その多くは、ヒューマンエラーが起因となって発生しているからです。そこで現在は当時の経験をセキュリティ対策に取り入れています。最前線にいる職員の対応1つで重大な事故につながりかねません。その代表例として4つのNGポイントをあげます。

(1) 紛失・置き忘れ

個人情報保存されたパソコンやUSBメモリーなどの媒体を社外に持ち出した際に起こりがちなトラブルです。個人情報が保存された媒体が入ったカバンを電車内等で置き引きされたことで発生しています。

(2) メールの誤操作

メールの送信ミスによって個人情報を含むメールが関係者以外に送信されてしまうトラブルです。個人情報が含まれた重要なファイルを間違えて添付したり、CcとBccを間違

[†] NHK 情報システム局/ICT-ISAC-JAPAN 事務局

"The Value of the Information Sharing in Cyber Attack Defense" by Toru Atsumi (Information Systems Department, NHK, Tokyo/Deputy Secretary General, ICT-ISAC-Japan, Tokyo)

表1 リスクマップ

	脅威検知レベル	対策判断者	対策の観点
レベル5	業務/サービス異常の検知	事業責任者/経営者	事業継続 (BCP)
レベル4	業務システム全体の健全性阻害の検知	リスク委員会CISO	システムの健全性
レベル3	内部ネットワークにおける異常拡散の検知/C&C対象	CSIRT	システムの安定性
レベル2	外部ネットワークの異常通信 (C&Cサーバ通信) の検知, 情報漏洩	SOC	影響範囲の特定
レベル1	内部ネットワークにおける通信変化を検知 (C&C通信の可能性)	NOC	被害の特定・除去
レベル0	外部ネットワークからのセキュリティ脅威の検知	ツール (機器)	被害の特定・除去

C&C: Command and Control CISO: Chief Information Security Officer
 CSIRT: Computer Security Incident Response Team SOC: Security Operation Center
 NOC: Network Operations Center BCP: Business continuity planning

えたりといった誤った解釈による致命的なミスがあります。

(3) 誤操作によるデータ削除

個人情報をはじめとする重要情報を誤って削除してしまうというケースです。個人情報を含む紙媒体の資料を他の資料と一緒に廃棄してしまったり、バックアップをとっていないデータを誤操作で削除してしまったりというトラブルがあります。

(4) 情報持ち出しルールの形骸化

個人情報の社外持ち出しを禁止している会社は多いはずですが、ところが、「ちょっとだけなら大丈夫だろう」と考えた社員が無断で個人情報を持ち出し、その後不注意が重なってしまうと、結果的に思わぬセキュリティトラブルにつながります。

いずれも社内ルールに違反していますが、「自分一人くらい」、「前回は大丈夫だった」などと言い訳をする者が多く、偶然にも悪い条件が重なった時、一人の小さなミスから、会社の信頼を失墜するほどの大事故につながってしまう恐れがあります。

4. 制御システムのセキュリティとリスクマップ

放送システムのように重要インフラを支える制御系システムでは、可用性を最大限に確保することが求められます。そのため運用にも大きな制約を伴い、可用性に影響する恐れがあれば、脆弱性の修正パッチを適用できないケースもあります。

また、制御系システムは外部脅威のリスクを考慮してクローズドなネットワーク環境で運用されますが、それゆえに万一マルウェアが侵入すれば、想定外の事態が起こり得る、非常に危険な環境だとも言えるのです。

こうした制御系システムの特性や課題を踏まえ、事業継続や評判も含めた各種リスクへの対応が必要であり、リスクの所在と、その対応をまとめたリスクマップを作成することをお勧めします(表1)。

まずは、システムが正常なのか異常なのか、異常な場合はその程度を明確にし、レベルごとに対策判断者と対策の観点を決めておきます。判断基準の作成に当たっては社員相互のコミュニケーション面を含め、部門をまたがる横断

的なリスクの洗い出しを行う必要もあります。こうしたアプローチにより、リスクが顕在化しても格段に適切な対応がとりやすくなります。

5. 事業者連携で先行対応につなげる

ICT-ISACではセキュリティ情報の共有を中核とし、他の組織に先行して脅威に対応できる仕組みを目指しています(図1)。現在は「サイバー攻撃者が圧倒的に有利」といわれます(図2)。セキュリティ脅威に関する情報やインテリジェンスを事業者同士で活用して、攻撃の成功を難しくさせ、リスクの低減につなげる取り組みです。

企業等がサイバー攻撃に迅速かつ効率的に対応するため、
攻撃情報を共有する業種毎の横連携組織

ISAC (Information Sharing and Analysis Center)

情報 共有 分析 センター

※情報セキュリティ会社は、攻撃情報と対策そのものが商品であるため、積極的に情報を他社と共有したり公開したりすることはしない。業種毎のセキュリティレベルを上げるため、企業側の情報共有組織が必要。

【設立】

1998年 アメリカでISACを大統領令により設置、現在19業界
 2002年7月 日本Telecom-ISAC Japan
 2014年8月 日本金融ISAC

図1 ISAC組織

【攻撃側】

攻撃者は企業内システムの脆弱性と弱点について攻撃してくる。
全体システムを把握しているため容易に繰り返し攻撃を仕掛けてくる。

VS

【防御側】

防御側は特定の端末、サーバ対応、対策に時間を使い、
全体の脆弱性対応などは後回しになったり、かなりの時間を使い安全な状態にしている。

どちらが有利な環境であるか？

圧倒的に攻撃者側が有利

図2 サイバー攻撃者が圧倒的に有利

6. ISACの必要性と機能

例えば、特定の同業会社を狙うようなサイバー攻撃では、攻撃者が効率的に実行するために、同じ手法を使う傾向があります(図3)。仮に、事業者ごとに攻撃を仕掛けられたタイミングが異なっても、ある事業者で検知した攻撃やその手法に関する情報をいち早く分析、共有して他の事業者の対策に反映できれば、被害抑止につながれるということです。

結果的に攻撃者が多大な時間や資金、人的リソースを費やして、標的ごとに異なる手法を開発しなければならず、

図3 ISACの必要性と機能

コスト増で割に合わない攻撃は実行しなくなることを狙っています。従来のセキュリティ対策は、脅威を防ぐことが重要とされ、「守る側」の視点にとらわれがちとの指摘もあります。私のアプローチは、「攻める側」の視点も取り入れることで、「守る側」の視点だけでは行き届かなかった対策の弱点を補完するものです。

しかし、このアプローチを実現するには、組織同士の信頼関係と密接な連携が欠かせず、人と人との信頼関係を組織と組織にも昇華できる取組みが必要になります。

7. むすび

サイバー攻撃への対応速度を上げるためには、今後は国内だけでなく海外も含め信頼できるコミッティへ組織として参加し、主体的に関わっていけるかどうか、重要なポイントです。発信のないところに情報は集まってきません。放送制御システムに限らず、広く制御システム全般に関する情報を収集、提供できるような仕組み作りが必要となってくるものと考えています。

(2018年2月9日受付)

熱海 徹 1978年、NHK入局。主に番組運行勤務、ハイビジョンスタジオ設備等の技術管理部門に従事。東京、仙台、山形を異動した。2013年より、情報システム局。主にイントラネットワークの運用に従事。2015年、情報セキュリティ対策グループを立ち上げ部門統括を行う。2016年より、(一社)ICT-ISAC-JAPANに出向し、現在、事務局次長。主に放送業界のセキュリティ全般についてまとめ役を行い、インシデント対応に従事。