

## 脆弱性対策は“いちごっこ”！

～どのように対処すべきか？～

### はじめに（脆弱性に関する誤った認識）

昨今、サイバー攻撃に関するニュース・記事が紙面を賑わす機会が増えている。企業がサイバー攻撃を受けた場合、システムダウンによる業務停止、情報漏えいによるレピュテーションの低下、さらには株価低迷・販売不振にまで発展するなど、経営に与える被害は極めて甚大である。

こうしたサイバー攻撃の糸口としては、様々な要因が考えられるものの、特に多い事由としては、脆弱性の悪用が挙げられる。脆弱性とは、製品におけるプログラムの不具合や開発者の意図しない処理など、セキュリティの棄損につながり得る欠陥のことを指す。サイバー犯罪者は脆弱性を悪用することで、攻撃対象のセキュリティの仕組みをすり抜け、冒頭に挙げたシステムダウンや情報窃取を行うことが可能となる。

脆弱性は、専門のソフトウェアやサービスを活用することで、開発段階で発見できるものもある。その一方で、それまでは問題がなかったとしても、情報システム内で使用されるソフトウェアやプログラムライブラリなどのバージョン更改や、ネットワーク・ハードウェアなどの技術進化によって、新たな脆弱性が発生するケースもあるため、完全に無くすことは困難である（「いちごっこ」が続いてしまうため）。

そのため、脆弱性への対策は企業にとっては憂慮すべき重要な課題である。このような状況を踏まえ、セキュリティ担当役員である A 氏の脆弱性に関する発言を見ていこう。



セキュリティ  
担当役員 A 氏

SNS で自社製品の脆弱性情報が拡散されているらしい。SNS なんぞどうせ一過性のものだろうし、気にしないでいいだろう。受付窓口もあるのに迷惑な投稿者だ...

半年前にわが社でも使用している製品の脆弱性が公開されたようだ。深刻度や影響度も不明だし、次回の IT 資産の定期棚卸のタイミングで考えればよいだろう

自社に組み込んでいる製品の脆弱性がベンダーから報告された。すぐに採用していることを公表した上で、セキュリティ部門に連携し適切な対応を取らせよう

上記の 3 つの発言には、勘違いと呼ぶべき内容が含まれている。それはどういった点だろうか、まずは、認識を合わせるために見ていきたい。

### SNS の拡散力に関する理解不足

ソーシャルメディアの拡散力は非常に強力なため、ネガティブな投稿内容の場合、その投稿を起点に炎上が発生し、企業のレピュテーションに多大な影響を及ぼす可能性があることを見落としている。

脆弱性のような経営被害につながる情報であれば尚更である。また、こうした SNS の拡散を見逃す、または、確認が遅れてしまう一因として、その企業に問合せ窓口が存在しない、または存在したとしても、そのことが世間に認知されていないケースも往々にして見られる。

ただし、こうした場合、投稿者は良かれと思い世間に知らしめる意味で、ソーシャルメディア上に公開する、という可能性も否定できない。そのため、一概に SNS に投稿されることを発信者側のモラル不足と捉えるのは危険な考え方である。

### 外部情報を活用したタイムリーな情報収集が不十分

脆弱性情報が公表された場合、セキュリティベンダーや研究者による対策検討が開始される一方で、攻撃者にとってもつけ込む手段の糸口を与えることになる。そのため、公開された瞬間からいかに早くそれをキャッチアップして、自社組織としての対策につなげるかが肝要となる。例えば、その動きが1か月後、3か月後、さらに長引いて半年後になるようではもはや致命的な事態を招きかねない。

また、脆弱性情報は必ずしも自社リソースのみで調査・分析しなければならないのだろうか。近年、脆弱性情報に関する様々な分析データを提供する外郭団体や専門機関が存在するが、そもそも、そういった情報を活用することはできなかったのだろうか。

### 不適切な報告タイミングと社内の連携不足

脆弱性情報を公表することは大切であるが、対策や影響範囲が不明瞭なまま公開すること前述したように攻撃者につけ込む糸口を与えてしまう。また、脆弱性情報はセキュリティ部門のみに連携するだけで良いのだろうか。

セキュリティ被害が発生した場合、単に技術的な分析・対応だけでなく、広報対応、監督官庁対応、顧客対応等、様々な外部ステークホルダーを見据えた対応が必要となる。つまり、セキュリティ管理を担う組織だけでなく、社内の様々な部門に影響が及ぶのではないだろうか。

以降では、上記の3つの問題点をどのように回避すべきかを解説する。

## 対策1：レピュテーションリスクのコントロール

ソーシャルメディア上で企業に関するネガティブな情報が拡散・炎上した場合、最終的には謝罪会見にまで発展する場合もある。そのため、企業にとってはソーシャルメディアを軽視することは、信用失墜を招きかねないことを認識する必要がある。そのためにも、ソーシャルメディアモニタリングの実施を推奨する。

ソーシャルメディアモニタリングとは、ソーシャルメディア上で企業の信用に影響を及ぼす発言の内容・傾向を監視することである。モニタリングにはアカウント、検索キーワード、そして監視を実施する担当者が必要となる。

アカウントは投稿内容の確認や投稿者とのコミュニケーションに必要であり、組織としての公式アカウントがある場合、それを活用するケースも見られる。検索キーワードとしては、主に製品名やサービス名が中心となる。当然ながら、海外でも展開している場合は日本語や英語のキーワードだけでなく、販売している国で使用される言語の製品名やサービス名も含めるべきである。そして、担当者がそれらのトピックに関する発言を定期的に確認し、レピュテーションに影響するようなネガティブな発言があれば、内容の確認や投稿者への連絡を行い、事態が収拾できるようコントロールする。ただし、モニタリングは多くのタスクが発生するため、社内で担当者をアサインできない場合、モニタリングサービスを専門とする企業への外部委託も検討すべきである。

ただし、上記は組織としてのプロアクティブな対応であるものの、その逆であるリアクティブな対応も重要となる。具体的には、問い合わせ窓口の設置・周知である。一般的には、公式ホームページ、SNS アカウントの詳細欄、または、脆弱性関連であれば脆弱性情報の共有コミュニティなど、複数のメディア上に掲載しておき、様々なシチュエーションでの問い合わせに応じる準備が重要となる。

さらに、外部からの連絡受付に際して、どのような情報を含めて欲しいか予め公開しておけば、情報不足による企業と報告者間での無駄なやり取りが発生することを防げる。

公開する情報媒体としては、ディスクロージャーポリシーや脆弱性対応ポリシーなどが挙げられる。通常それらのポリシーには、共有された情報に関する企業の対応方針が記載されており、その中には脆弱性発見のためのテスト方法や制限事項、対象製品、連絡窓口や連絡時に必要な内容、対応プロセスといった情報が含まれる。これらの内容を事前に確認してもらうことで、企業と報告者の間でのよりスムーズなやり取りが可能となるだろう。

Commissioners	Vulnerability Disclosure Policy
Contact	The U.S. Securities and Exchange Commission ("SEC") is committed to maintaining the security of our systems and protecting sensitive information from unauthorized disclosure.
Data	
Divisions and Offices	This policy describes what systems and types of security research are covered under this policy, how to send us vulnerability reports, and how long we ask security researchers to wait before publicly disclosing vulnerabilities.
Regional Offices	We encourage security researchers to contact us to report potential vulnerabilities identified in SEC systems. For reports submitted in compliance with this policy, the SEC will acknowledge receipt within three business days, endeavor to timely validate submissions, implement corrective actions if appropriate, and inform researchers of the disposition of reported vulnerabilities.
Division and Office Directors	
Firms	If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and we will not recommend or pursue legal action related to your research.
Privacy and Security	
Reports and Publications	<b>Test Methods</b> <b>Security researchers must not:</b> <ul style="list-style-type: none"><li>• Test any system other than the systems set forth in the "Scope" section below,</li><li>• disclose vulnerability information except as set forth in the "Reporting a Vulnerability" and "Disclosure" sections below,</li><li>• engage in physical testing of facilities or resources,</li></ul>
Securities Laws	
Upcoming Events	
What We Do	

図1 ディスクロージャーポリシーの例

<https://www.sec.gov/vulnerability-disclosure-policy>

## 対策 2：外部情報の最大限の有効活用

脆弱性は公表されて間もなく、サイバー攻撃に悪用されることも多いため、随時情報をキャッチアップすることが求められる。脆弱性情報の収集には、Web サイトの更新を通知してくれる RSS（Really Simply Syndication）や、特定のトピックに関する情報を指定した頻度で通知してくれる Google アラートと言った外部ツールを活用することも可能であり、ツールの扱いに慣れればすぐに始められるだろう。

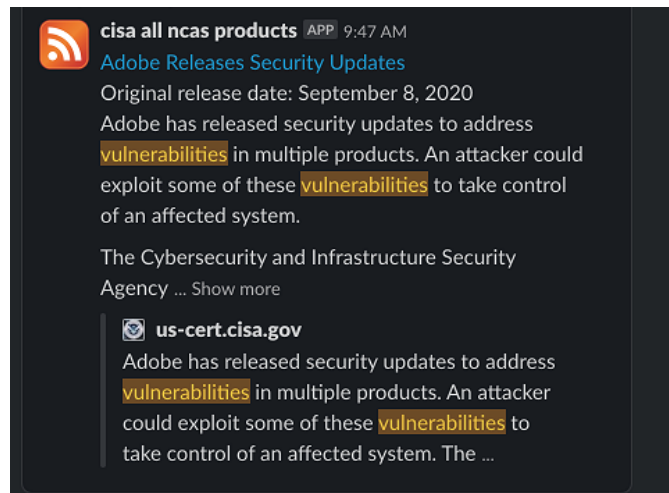


図 2 RSS による Web サイト更新の通知例

もちろん、IT 資産の刷新や棚卸に合わせて脆弱性情報を収集しているケースもあると推定される。しかし、いち早く脆弱性情報を認識することで、通常運用を妨げることがない修正スケジュールや人的リソースの確保、さらにはセキュリティ製品による監視強化など、事前に脆弱性への対策を練ることが可能となる。

また、脆弱性情報は、外郭団体（IPA や JPCERT/CC など）や製品ベンダー、セキュリティベンダーから随時発信されている。公表される脆弱性の多くには脆弱性評価のため、CVSS（共通脆弱性評価システム）によるスコアが記載されている。CVSS では、情報セキュリティの CIA（機密性、完全性、可用性）、攻撃可能性、影響範囲など複数の観点から、0（影響無し）～10（緊急の対応が必要）のレンジで算出されるため、脆弱性の深刻度判定の参考になりうる。

加えて、ベンダーから公表される脆弱性の回避策・緩和策は、修正にかかる工数や時間の目途をつける参考になるだろう。例えば、深刻度の高い脆弱性が確認され、自社で利用している製品が影響を受ける場合は、IT 部門にその旨を連携することで、対応可否や対応期限の判断に活用できるだろう。

## 対策 3：公表タイミングと社内連携の重要性

脆弱性情報の公表は、早ければよいとは限らない。対策や影響範囲が不明瞭な状況下でむやみに公表することで、攻撃者にとってのヒントやさらなる攻撃を促進し、結果として、サイバー攻撃の被害者となる可能性も高い。そのため、公表前には以下の情報が揃っているかを最低限確認する必要がある。

- 脆弱性の詳細
- 影響範囲に関する情報（影響を受ける製品など）
- 回避策・緩和策に関する情報
- 問い合わせ窓口

上記の情報を網羅的に揃えるには、社内関係者との連携が必須である。社内関係者は開発、営業、サポート、法務部門と多岐にわたるため、体制構築時には連携の中心を担う「調整チーム」を設置するのが望ましい。

各部門が各々で情報連携を行うのではなく、「調整チーム」とのコミュニケーションに一本化することにより、必要最低限のリソースで脆弱性対応が期待できる。

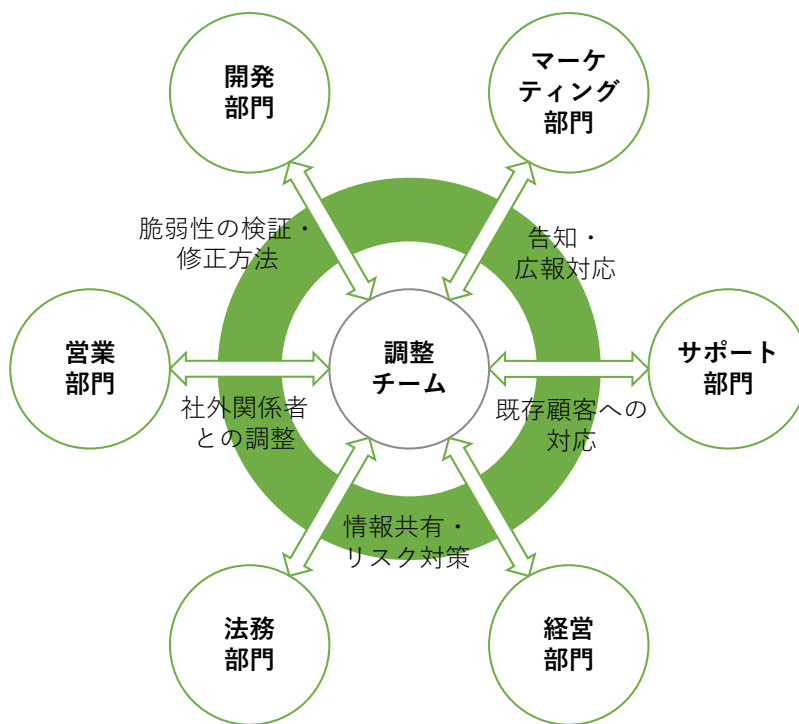


図3 調整チームを中心とした社内連携例

「調整チーム」はその位置づけから、関係部門の業務を理解している人材で構成されていることが望ましく、CSIRT（Computer Security Incident Response Team）はその一例として挙げられる。CSIRTは、コンピュータセキュリティに関わるインシデントに対処・発生予防・社内外調整をすることを目的に設置されるチームであるため、「調整チーム」に適していると考えられる。また、「調整チーム」以外の各部門においても、脆弱性対応時の担当者を設置し、確認事項や意思決定者の一覧、承認プロセスなどの対応フローを予め準備することで、より連携スピードを速められるだろう。

## 終わりに

以上の解説を踏まえると、冒頭のA氏の発言は以下になることが望ましい。



SNSのモニタリング担当者に投稿の詳細を確認して、対応が必要か判断しよう。脆弱性情報の受付窓口も分かりづらいようだからもっと目立つ場所に案内を設置・周知しよう

外部の専門機関の公開情報を参考にとすると、今回の脆弱性の深刻度はそこまで高くないから対応は必要なさそうだ。今後はタイムリーに脆弱性情報を収集し、迅速な対応につなげよう

各部門の考察はどうなっている？必要な情報がまだ揃っていないのならば、公表は一旦控えよう。まずは、社内の関係部門を交えた協議を推進するためにも、調整チーム主導の下、全社的な調整を進めよう

脆弱性を完全に無くすことは不可能である。「いたちごっこ」は続くだろう。ただし、発生した脆弱性に対して、適切かつ迅速に対応することで、被害は極小化できると考えられる。そのためにも、レピュテーションリスクのコントロール、外部情報の有効活用、公表タイミング検討および社内連携体制の構築は、重要な成功要因であり、こうした取組みを組織一丸となつて行うことを期待したい。

## デロイトトーマツサイバー合同会社

Mail [ra\\_info@tohatsu.co.jp](mailto:ra_info@tohatsu.co.jp)

URL [www.deloitte.com/jp/dtcy](http://www.deloitte.com/jp/dtcy)

【国内ネットワーク】 東京・名古屋・福岡

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が

要求される場合、本サービス 内容がご提供できない可能性があります。詳細はお問合せください。

デロイトトーマツグループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイトトーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイトトーマツコンサルティング合同会社、デロイトトーマツファイナンシャルアドバイザー合同会社、デロイトトーマツ税理士法人、DT 弁護士法人およびデロイトトーマツコーポレートソリューション合同会社を含む）の総称です。デロイトトーマツグループは、日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザー、コンサルティング、ファイナンシャルアドバイザー、税務、法務等を提供しています。また、国内約 30 都市以上に 1 万人を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイトトーマツグループ Web サイト（[www.deloitte.com/jp](http://www.deloitte.com/jp)）をご覧ください。

Deloitte（デロイト）とは、デロイトトウシュトーマツリミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよびそれらの関係法人はそれぞれ法的に独立した別個の組織体です。DTTL はクライアントへのサービス提供を行いません。詳細は [www.deloitte.com/jp/about](http://www.deloitte.com/jp/about) をご覧ください。デロイト アジア パシフィック リミテッドは DTTL のメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける 100 を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザー、リスクアドバイザー、税務およびこれらに関連するプロフェッショナルサービスの分野で世界最大級の規模を有し、150 を超える国・地域にわたるメンバーファームや関係法人のグローバルネットワーク（総称して“デロイトネットワーク”）を通じ Fortune Global 500® の 8 割の企業に対してサービスを提供しています。“Making an impact that matters”を自らの使命とするデロイトの約 312,000 名の専門家については、（[www.deloitte.com](http://www.deloitte.com)）をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性があります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

Member of  
**Deloitte Touche Tohmatsu Limited**

© 2020. For information, contact Deloitte Tohmatsu Cyber LLC.