B2 脆弱性管理をみんなで議論しよう！

Internet Week 2024 BoF / 2024-11-25

株式会社ラック
次世代セキュリティ技術研究所
井上　圭

Agenda

1. 運用における脆弱性管理の振り返り
2. ディスカッション1
3. 今後求められる、脆弱性管理
4. ディスカッション2

Profile

井上 圭

株式会社ラック
サイバーグリッドジャパン
次世代セキュリティ技術研究所
兼　サイバーセキュリティプラットフォーム開発企画部 企画

セキュリティ運用、特に脆弱性管理について、研究や講演を実施。
近年は、ソフトウェア業界から見たサプライチェーンセキュリティや
SBOMについても対象としている。
また、JNSAの会員として、学生教育等も実施している。

最近の発表

- CodeBlue 2022 OpenTalks
- Janog 52 CFP
- Internet Week 2023 C6
- NCA Annual Conference 2023 車座1
- NCA Annual Conference 2023 CFP
- OWASP Nagoya Chapter/OWASP 758 Day
- Hardening Designers Conference 2024 Session4
- Internet Week Showcase in 福岡
- Internet Week 2024 D1-2
- 他

所属団体

- 日本ネットワークセキュリティ協会（JNSA）
  - ✓ 社会活動部会
  - ✓ 教育部会
- 日本セキュリティオペレーション事業者協議会（ISOG-J）
  - ✓ WG1”脆弱性トリアージガイドライン作成の手引き”
  - ✓ WG6”セキュリティ対応組織の教科書”
- 日本シーサート協議会（NCA）
  - ✓ インシデント対応演習訓練WG
  - ✓ 脆弱性管理WG
- セキュリティトランスペアレンシーコンソーシアム
- 他

01

運用における脆弱性管理の振り返り

対応フロー

一般的な脆弱性管理について述べます。
おおよそ下記のようなフローが想定されています。

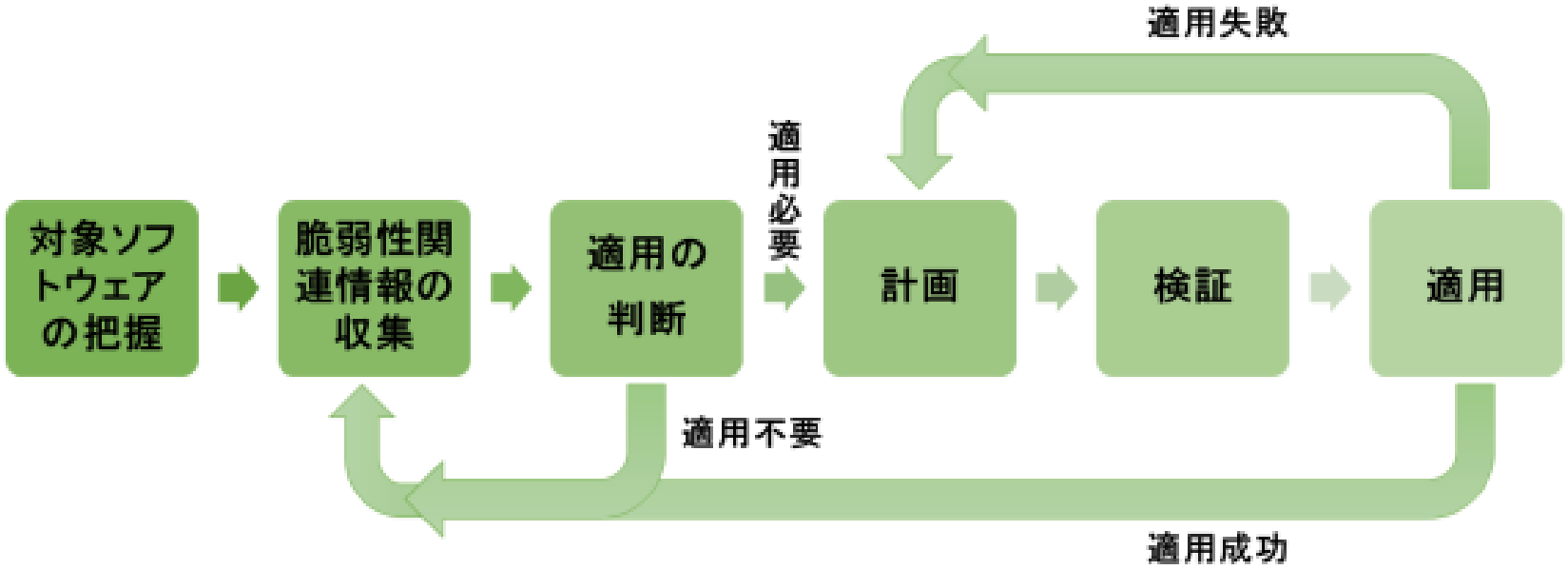
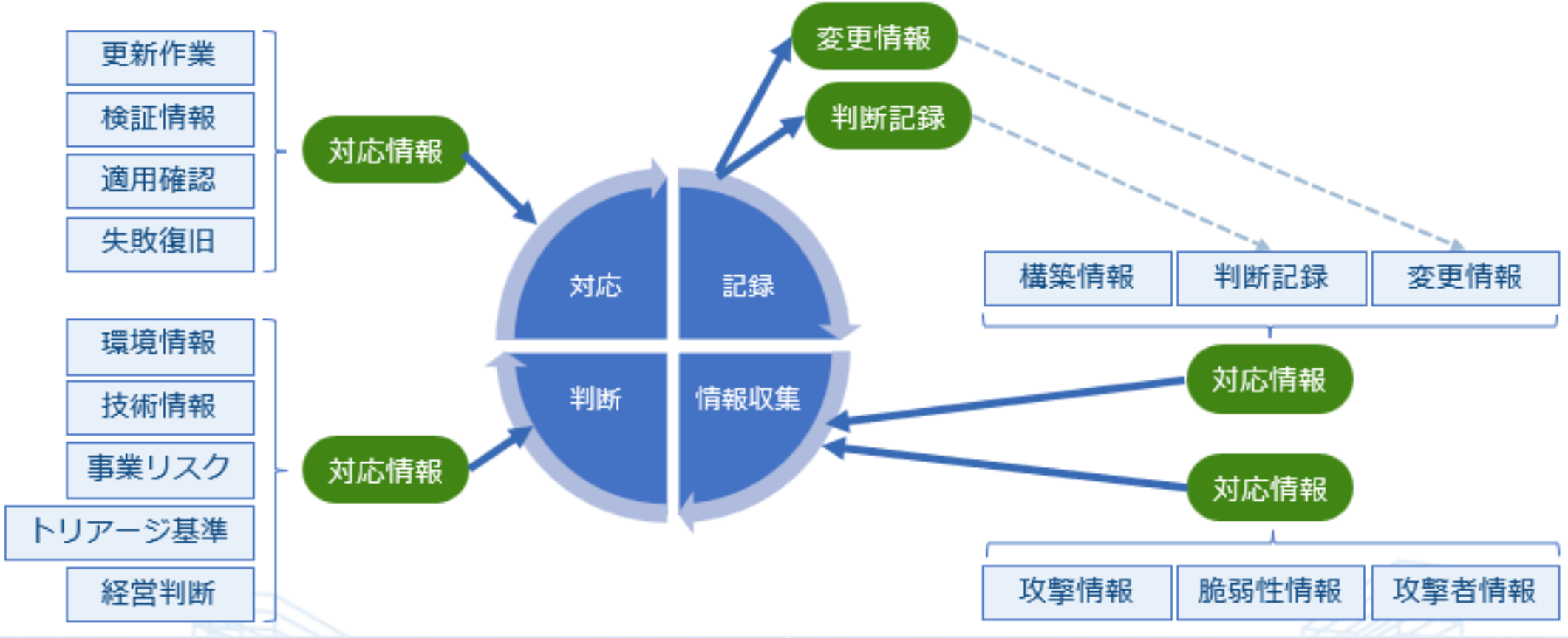


図 2-1-1　脆弱性対策のフロー

IPAテクニカルウォッチ「脆弱性対策の効果的な進め方（ツール活用編）」より引用
https://www.ipa.go.jp/security/reports/technicalwatch/20190221.html

対応フロー；詳細

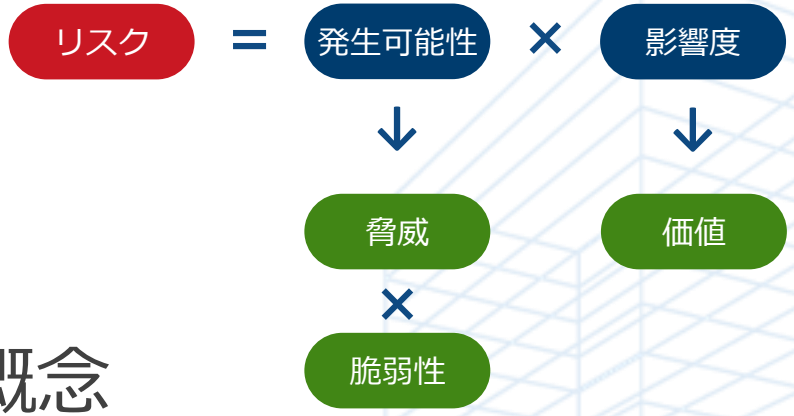
前述のものは2019年の資料であり、近年の状況を踏まえてより詳しく見ると、以下のようになると考えます。

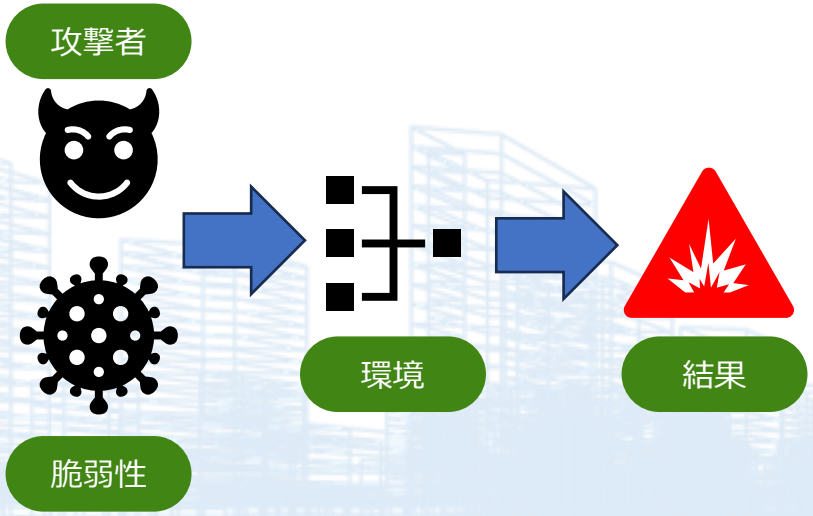


脆弱性トリアージ

全ての脆弱性に対応することは難しいため、優先順位付けを行います。

- 対応することは難しい
  ＝「すべて同時に」対応することは難しい
  ＝やらなくていいわけではない
- 脆弱性対応＝事業リスクへの対策、という概念





フレームワーク	概要	リスク / 発生可能性 / 価値
CVSS	脆弱性それ自体の影響	脆弱性
EPSS	脆弱性の発生確率	脅威
KEV Catalog	脆弱性の悪用状況	脅威、脆弱性
vulnrichment	脆弱性の追加情報	脅威、脆弱性
SSVC	トリアージフレームワーク	リスク

02

ディスカッション1
：運用における脆弱性管理の振り返り

ディスカッション

このような運用、うまくいく組織と、うまくいかない組織があります。

これらのフローやトリアージについて、議論しませんか？

- 何か質問や意見があれば、挙手ください
- ある程度の時間までディスカッションしましょう。BoFの楽しみの一つです。

例えば、、、

- 脆弱性情報の収集、粒度がうまく合わない問題
- 脆弱性トリアージをするには、残存脆弱性が多すぎる
- 自動化と人間による決断の役割分界点はどうしよう

03

今後求められる、脆弱性管理

SBOMや他国の標準に合わせて

ここ数年の話題として「SBOMで脆弱性管理をする」という話が出ています。

- 主に、製造業（特に車や医療系）は「必要に駆られて」進めています。
- 他方、WEB等ソフトウェア事業者においては…

そして、その延長線上として「サプライチェーンセキュリティ対応」が話題になってきています。

- EU CRA（サイバーレジリエンス法）などで、ソフトウェア設計段階からのセキュリティが求められています。

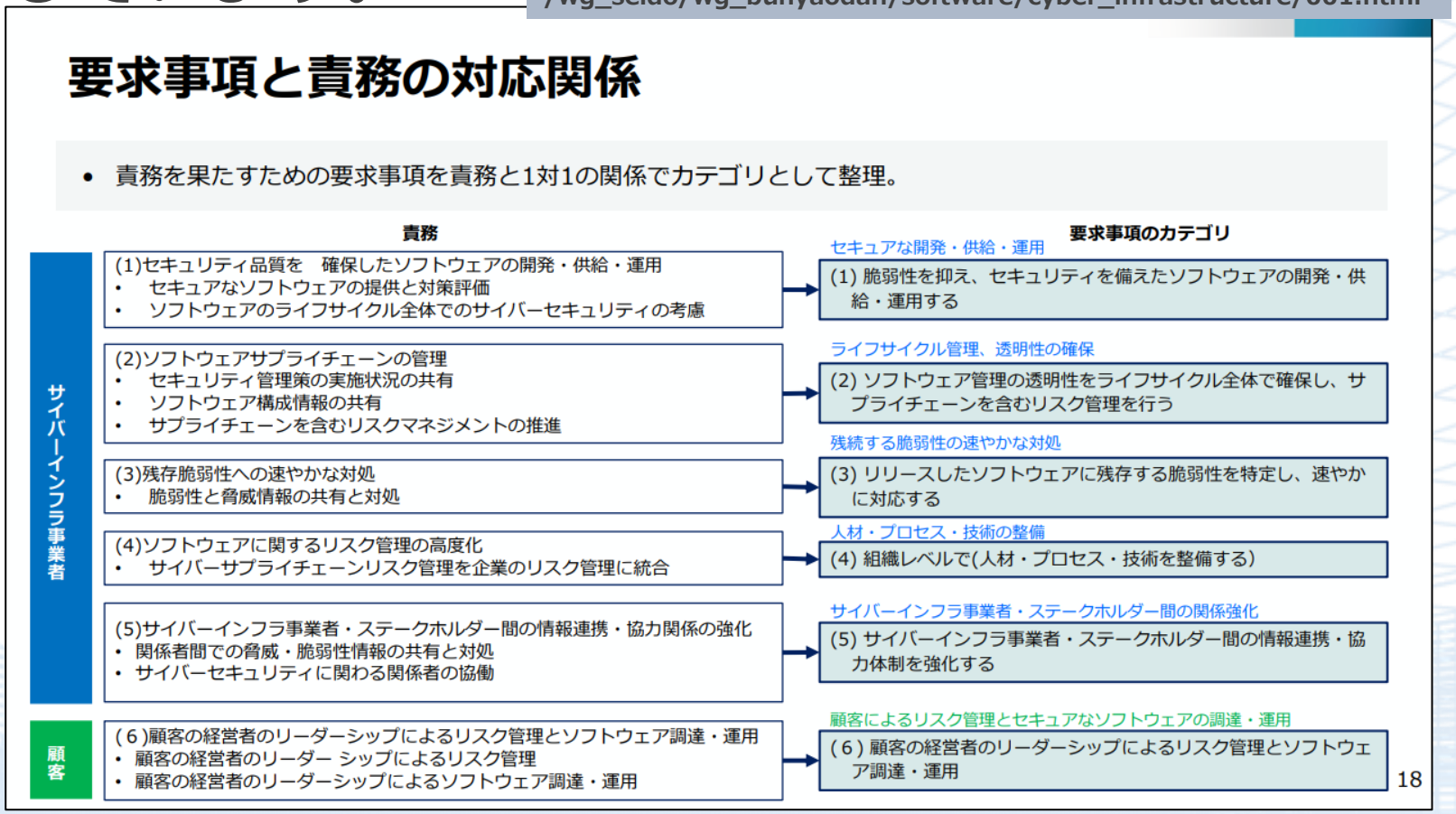
経済産業省の取組

「サイバーインフラ事業者に求められる役割等の検討の方向性」として議論が2024/09に始まり、政府調達や重要インフラの調達の要件に今後しようとしています。

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/cyber_infrastructure/001.html

まだ議論中と思われる資料から抜粋。

- 開発プロセス
  - セキュリティ教育
- 開発時
  - 脅威モデリング等の実施
  - セキュアビルド
- リリース後
  - 継続的な脆弱性対応、リリース、通知
- 協力体制
  - コミュニティへの参加



要求事項と責務の対応関係

- 責務を果たすための要求事項を責務と1対1の関係でカテゴリとして整理。

	責務	要求事項のカテゴリ
サイバーインフラ事業者	(1)セキュリティ品質を　確保したソフトウェアの開発・供給・運用 • セキュアなソフトウェアの提供と対策評価 • ソフトウェアのライフサイクル全体でのサイバーセキュリティの考慮	セキュアな開発・供給・運用 (1) 脆弱性を抑え、セキュリティを備えたソフトウェアの開発・供給・運用する
	(2)ソフトウェアサプライチェーンの管理 • セキュリティ管理策の実施状況の共有 • ソフトウェア構成情報の共有 • サプライチェーンを含むリスクマネジメントの推進	ライフサイクル管理、透明性の確保 (2) ソフトウェア管理の透明性をライフサイクル全体で確保し、サプライチェーンを含むリスク管理を行う
	(3)残存脆弱性への速やかな対処 • 脆弱性と脅威情報の共有と対処	残続する脆弱性の速やかな対処 (3) リリースしたソフトウェアに残存する脆弱性を特定し、速やかに対応する
	(4)ソフトウェアに関するリスク管理の高度化 • サイバーサプライチェーンリスク管理を企業のリスク管理に統合	人材・プロセス・技術の整備 (4) 組織レベルで(人材・プロセス・技術を整備する)
	(5)サイバーインフラ事業者・ステークホルダー間の情報連携・協力関係の強化 • 関係者間での脅威・脆弱性情報の共有と対処 • サイバーセキュリティに関わる関係者の協働	サイバーインフラ事業者・ステークホルダー間の関係強化 (5) サイバーインフラ事業者・ステークホルダー間の情報連携・協力体制を強化する
顧客	(6)顧客の経営者のリーダーシップによるリスク管理とソフトウェア調達・運用 • 顧客の経営者のリーダー シップによるリスク管理 • 顧客の経営者のリーダーシップによるソフトウェア調達・運用	顧客によるリスク管理とセキュアなソフトウェアの調達・運用 (6) 顧客の経営者のリーダーシップによるリスク管理とソフトウェア調達・運用

18

要求事項の概要

サイバーインフラ事業者に求められる役割等の検討の方向性
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/cyber_infrastructure/pdf/001_04_00.pdf

- 要求事項のカテゴリは、複数のステートメント（要求事項の具体的な取組の在り方）から構成する。

	要求事項のカテゴリと概要	ステートメント
サイバーインフラ事業者	(1) セキュアな開発・供給・運用 脆弱性を抑え、セキュリティを備えたソフトウェアを開発・供給・運用する	(1)-1 設計時のリスク評価と対策の追跡 (1)-2 セキュアなビルド (1)-3 テスト (1)-4 サービスのモニタリング
	(2) ライフサイクル管理、透明性の確保 ソフトウェア管理の透明性をライフサイクル全体で確保しサプライチェーンを含むリスク管理を行う	(2)-1 セキュアなコンポーネントの調達 (2)-2 リリースファイルやデータのセキュアなアーカイブ (2)-3 関係者間のセキュリティ要件の確立 (2)-4 利用者への適切な情報提供
	(3) 残続する脆弱性の速やかな対処 リリースしたソフトウェアに残存する脆弱性を特定し、速やかに対応する	(3)-1 継続的な脆弱性調査 (3)-2 検知した脆弱性への対処 (3)-3 対処結果を組織のプロセス改善に活用
	(4) 人材・プロセス・技術の整備 組織レベルでソフトウェアに関わる人材・プロセス・技術を整備する	(4)-1 人材：人員の整備 (4)-2 プロセス：開発ポリシーの確立と法令順守 (4)-3 プロセス：運用ポリシーの確立と法令順守 (4)-4 プロセス：開発運用基準の策定 (4)-5 技術：セキュアな開発ツールの整備 (4)-6 技術：セキュアな開発環境の整備
	(5) サイバーインフラ事業者・ステークホルダー間の関係強化 サイバーインフラ事業者・ステークホルダー間の情報連携・協力体制を強化する	(5)-1 情報連携のための組織体制 (5)-2 協力体制の強化
顧客	(6) 顧客によるリスク管理とセキュアなソフトウェアの調達・運用 顧客の経営者のリーダーシップによるリスク管理とセキュアなソフトウェア調達、運用を行う	(6)-1 顧客の経営者のリーダーシップによるリスク管理 (6)-2 顧客の経営者のリーダーシップによるソフトウェアの調達、運用

19

04

ディスカッション2
：今後求められる、脆弱性管理

ディスカッション

確かに、欧米の法体系ではサプライチェーンセキュリティの対策が求めれています。

ゴールは間違っていないようには見えます。しかしながら、今すぐに対応できるかといえば、そうではないように思えます。

私たちはどこまで対応できそうでしょうか。どうしましょうか。

- SBOMは、そもそも資産管理リストであって、脆弱性管理のためのものではない（たまたまそれに利用できる）んだよなぁ
- 重要インフラ等はやってくれていいけど、SaaSサービス業者等はSBOMだけ出しておけばいいのかしら。そもそもSBOMの依存関係は何階層まで？
- そもそものベストプラクティスを提示してもらう必要があるのでは？開発から運用 - サービス終了までのベストプラクティスがあり、それに則る、みたいな形にしないと普及？しないのでは？
- Etc…

おわりに

私からのセッションは以上となります。

「今」の脆弱性管理と「今後」の脆弱性管理について、何らかの視点が得られたのであれば幸いです。

次は株式会社YONA 三国様から、インシデント対応をしている現場目線から見える脆弱性管理についてお話しいただきます。
その後、株式会社ハートビーツ 伊藤様から、運用の視点でお話を頂きます。

異なる視点で見えることをお話しいただきつつ、それを基にした議論ができればと考えています。

Thank you!

Any Question?

※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。
※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。
※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。