

これからの脆弱性管理

～SBOMだけじゃないサプライチェーンセキュリティに
求められるものとは～


京都産業大学情報理工学部ランチタイムトーク x OWASP Kansai (20241228)

株式会社ラック
次世代セキュリティ技術研究所
井上圭
kei.inoue@lac.co.jp



本日は、最近話題になっている「サプライチェーンセキュリティ」について、現状とこれからについてお話ししようと思います。

サプライチェーンセキュリティと言っても、
「サプライチェーンを通して攻撃を受けた（サプライチェーン攻撃）」の話ではなく、
「製造過程におけるサプライチェーン全体でのセキュリティ確保」の範囲の話をします。

- サプライチェーン攻撃
 - サプライチェーン上に脆弱な取引先を侵害し、ターゲット企業への侵害を行う
- 製造過程におけるセキュリティ確保 
 - 製品製造過程における、情報の透明性の確保（トランスペアレンシー）
 - どのようなソフトウェア/バージョンが使われているか、適切にビルドされたものであることの証明、等

井上 圭



kei.inoue@lac.co.jp

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統括部 企画

非IT企業情報システム部、MSP（Managed Service Provider）、セキュリティコンサルタントなどを経験し、2024年07月にラックに入社。脆弱性管理やセキュリティ運用について研究や講演を行い、確かなテクノロジーで「信じられる社会」を目指す。

最近の発表

- CodeBlue 2022 Open Talks
- Janog 52 CFP
- Internet Week 2023 C6
- NCA Annual Conference 2023 車座1, CFP
- OWASP Nagoya Chapter/OWASP 758 Day
- Hardening Designers Conference 2024 Session4
- Internet Week SHOWCASE in 福岡
- Internet Week 2024 D1-2, BoF
- NCA Annual Conference 2024 CFP1, CFP2
- 他

参加団体

- 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ための手引き”
 - 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（STコンソーシアム）
- 他

Agenda

1. 今までのサプライチェーンセキュリティ
2. 求められているサプライチェーンセキュリティ
3. 現在想定されている方法論
4. まとめ

Appendix

01 今までの サプライチェーンセキュリティ

近年、サプライチェーンの侵害によるインシデントが増えています。
例えば以下のようなものがありました。

- Lineヤフーの個人情報漏洩
 - 中国NAVER Cloudが委託する企業で従業員PCがマルウェアに感染、同端末がLINEヤフーとNAVER Cloudの従業員情報を扱う共通の認証基盤で管理するネットワークに接続が許可されていた。
 - 個人情報44万件の流出。
- Apache Log4j/Log4shell
 - 遠隔で任意の処理を実行できる脆弱性が発見されたが、様々なソフトウェアに組み込まれていたことから発見/追跡/改修が困難。
- SolarWinds
 - 正規のソフトウェアアップデートが改ざんされ、利用組織全体に侵害されたソフトウェアが配布された。
- その他多数

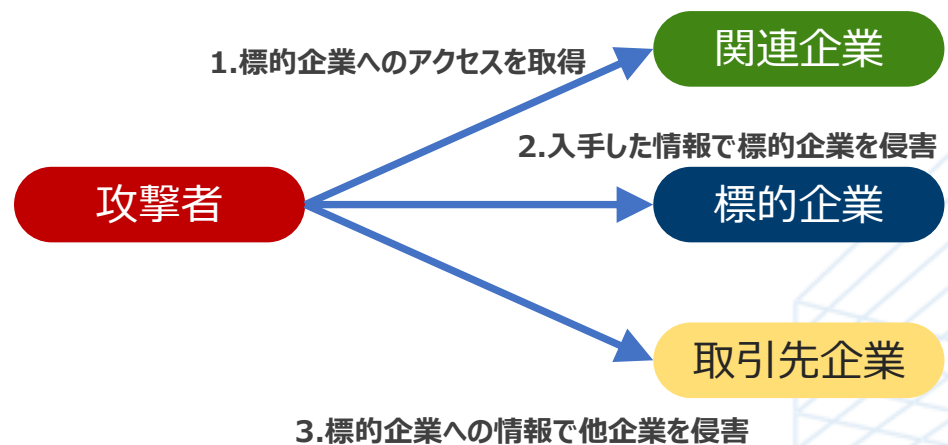


サプライチェーンの話が出ると、おおよそ2つの文脈が存在します。
あまり意識されていないことが多いので、補足しておきます。

- **企業活動** におけるサプライチェーン
 - 取引先のマルウェア感染から影響を受ける（Emotet等）
 - 委託先の侵害により、委託元が侵害される（Lineヤフー等）
- **製品/サービス** におけるサプライチェーン
 - 自社で開発していない部分の脆弱性の影響を受ける（Log4j等）
 - 正規のソフトウェアアップデートが改ざんされる（SolarWinds等）
 - = 脆弱性管理に関連する部分

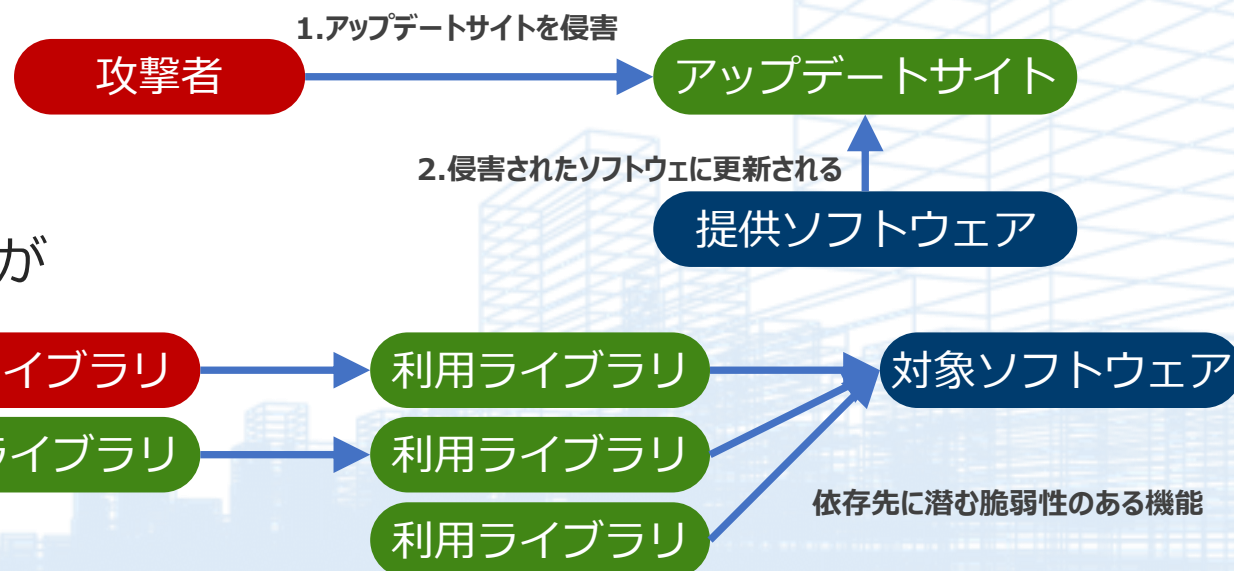
今回は、後者の「製品/サービスにおけるサプライチェーン」の話をします。

標的企業よりもセキュリティ対策が手薄な
関連企業等を侵害し、そこで得た標的企業
へのアクセス情報などを基に攻撃を行います。



ソフトウェアアップデート先を侵害し、アップ
デートのためにアクセスしたソフトウェアを
侵害されたものに置き換える攻撃もあります。

(SolarWinds)



攻撃ではないですが、ソフトウェアの依存関係が
複雑になり、依存先に潜む脆弱性が
版ベンツ困難になっています。

(Log4Shell)

サプライチェーンセキュリティの文脈では、業界/業種により状況がが違うように見えます。

現状だと、以下のように見えます。

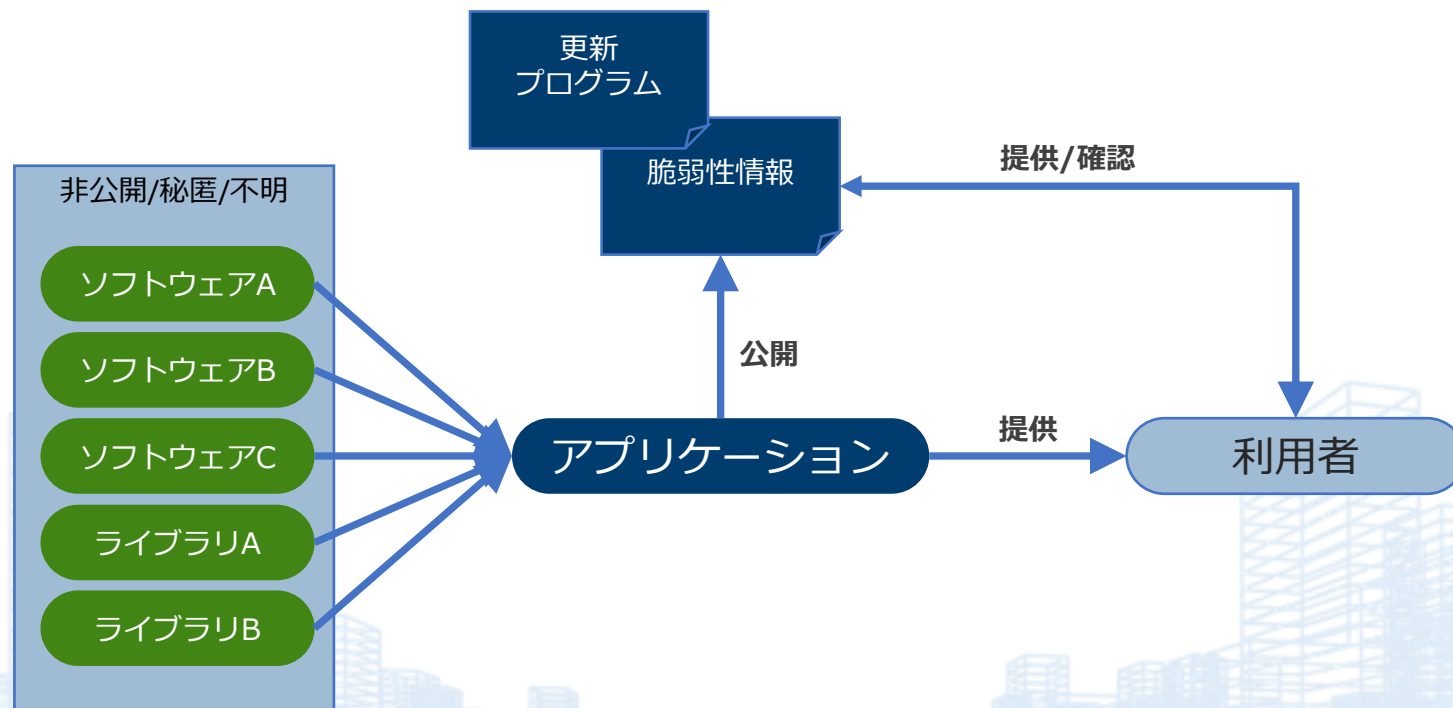
- 製造業（自動車や医療など）
 - 法的にサプライチェーン対応が求められている
 - SBOMなどは、必要だから実施しており、無いと開発に影響が出る
- IT/WEB/ソフトウェア産業
 - 法的にサプライチェーン対応が求められているわけではない
 - SBOMなどは、脆弱性管理の延長線上でしかない
 - その時点で最新版/動くもの、という概念が強いように感じる

製品製造自体で
必要としている

セキュリティ対策で
必要とされている

上記のような差があるため、業界一律でサプライチェーンセキュリティ対策のベストプラクティスを策定することが難しい状況となっています。

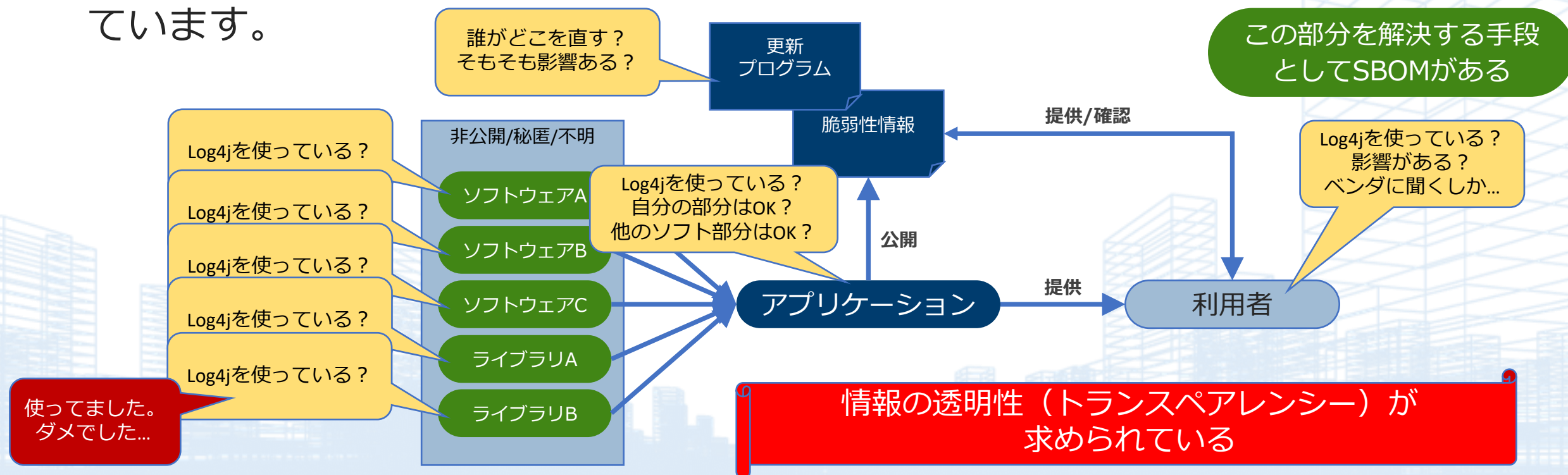
ソフトウェア業界では、あまりサプライチェーンを意識されることは無いような状況でした。



提供するベンダ/サプライヤの情報に頼る状況

どのようなソフトウェアが使われているかが不透明なため、例えばLog4Shellの脆弱性の場合は「利用している製品は影響を受けるのか」「製品で利用しているソフトウェアは影響を受けるのか」などの把握が困難、且つだれがいつどう対応するのかが不透明な状況がありました。

これらに対応する必要があり、サプライチェーンセキュリティが今進められています。



02 求められている サプライチェーンセキュリティ

諸外国でもサプライチェーンセキュリティ確保のために法制化が始まっています。

TLP: CLEAR

- まずは政府機関が調達するソフトウェア等について、対応を求めている
 - 米国
 - OMB覚書M22-18（2022/09）で、SSDFの実装の自己適合証明を確認することを要求
 - 米軍においては、2025年02月以降はSBOMを求める予定
 - 英国
 - Code of Practice for Software Vendorsで、セキュアな設計開発などの行動規範を示す
 - EU
 - Cyber Resilience Actで、セキュリティを考慮した設計、開発の評価や適合証明を義務化

ソフトウェアサプライチェーンに関わる諸外国の取組	
<ul style="list-style-type: none">• 欧米を中心に、ソフトウェアサプライチェーンにおける脆弱性対策に関わる制度、ガイドライン類の整備が進む。• セキュア・バイ・デザイン/デフォルトの概念が広まっており、サイバーインフラ事業者には、顧客との適切な役割分担のもと、自社が提供するソフトウェア製品のサイバーセキュリティ対策が求められている。	
欧州	
EU Cyber Resilience Act	<ul style="list-style-type: none">• デジタル要求を満たした全ての製品（ソフトウェア含む）の製造者に対し、セキュリティを考慮した設計、開発の評価や適合証明書を義務化。• 2024年後半に発効見込み。報告義務を除き、2027年夏頃運用開始を想定。
英国	
Code of Practice for Software Vendors	<ul style="list-style-type: none">• ソフトウェアサプライチェーン攻撃等のリスクに対処するためのソフトウェアベンダー向けの行動規範。セキュアな設計開発、セキュアな開発環境、セキュアな導入と保守、顧客とのコミュニケーションの原則から構成。• 2024年公表。
Guidelines for secure AI system development	<ul style="list-style-type: none">• セキュアバイデザインの観点から、ソフトウェアのうち AI に焦点を当て、AI セキュアな AI システムの構築を支援するための指針を整理。• 2023年発表。内閣府科学技術・イノベーション推進事務局及び内閣サイバーセキュリティセンターも署名。
ソフトウェアサプライチェーンに関わる諸外国の取組（つづき）	
米国	
NSA SECURING THE SOFTWARE SUPPLY CHAIN / Recommended Practices Guide	<ul style="list-style-type: none">• 供給者、開発者、顧客の3部構成となっており、セキュアなソフトウェアサプライチェーンを確保するために各主体に推奨されるプラクティスを整理。• 2022年発行。
NIST SP800-218	<ul style="list-style-type: none">• ソフトウェア開発者向けに、ソフトウェアライフサイクル全体でセキュアなソフトウェアを開発するためのフレームワーク（Secure Software Development Framework : SSDF）。• 2022年発行。
OMB M-22-18（M-23-16に更新）	<ul style="list-style-type: none">• 政府機関が、ソフトウェアベンダーに対して、SSDFの実装の適合性を証明する自己適合宣言書の取得を要求することを定める文書。自己適合宣言書では、SP800-218から抽出した最低限とするセキュアなソフトウェア開発プラクティスに従っていることを宣言。• 2023年発行。
Supply Chain Cybersecurity Principles	<ul style="list-style-type: none">• 米国のエネルギー事業者とそのサプライヤー向けのサプライチェーン・サイバーセキュリティ原則。• 2024年公表。
Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default	<ul style="list-style-type: none">• ソフトウェア開発事業者が脆弱なソフトウェアを商品化しないよう、そして顧客にセキュリティ確保の負担をできるだけ負わせないようにすることを目指し、セキュア・バイ・デザイン/デフォルトの概念に基づき、ソフトウェア開発事業者に求められる3つの原則を整理。• 2023年発行。内閣サイバーセキュリティセンターとJPCERTも署名。

ソフトウェアサプライチェーンに関わる諸外国の取組

- 欧米を中心に、ソフトウェアサプライチェーンにおける脆弱性対策に関わる制度、ガイドライン類の整備が進む。
- セキュア・バイ・デザイン／デフォルトの概念が広まっており、サイバーインフラ事業者には、顧客との適切な役割分担のもと、自社が提供するソフトウェア製品のサイバーセキュリティ対策が求められている。

欧州

EU Cyber Resilience Act

- デジタル要素を備えた全ての製品（ソフトウェア含む）の製造者に対し、**セキュリティを考慮した設計、開発の評価や適合証明書を義務化**。
- 2024年後半に発効見込み。報告義務を除き、2027年夏頃運用開始を想定。

英国

Code of Practice for Software Vendors

- ソフトウェアサプライチェーン攻撃等のリスクに対処するためのソフトウェアベンダー向けの行動規範。**セキュアな設計開発、セキュアな開発環境、セキュアな導入と保守、顧客とのコミュニケーション**の原則から構成。
- 2024年公表。

Guidelines for secure AI system development

- **セキュアバイデザインの観点**から、ソフトウェアのうち AI に焦点を当て、A セキュアな AI システムの構築を支援するための指針を整理。
- 2023年発表。内閣府科学技術・イノベーション推進事務局及び内閣サイバーセキュリティセンターも署名。

ソフトウェアサプライチェーンに関わる諸外国の取組（つづき）

米国	
NSA SECURING THE SOFTWARE SUPPLY CHAIN / Recommended Practices Guide	<ul style="list-style-type: none">• <u>供給者、開発者、顧客</u>の3部構成となっており、セキュアなソフトウェアサプライチェーンを確保するために各主体に推奨されるプラクティスを整理。• 2022年発行。
NIST SP800-218	<ul style="list-style-type: none">• ソフトウェア開発者向けに、<u>ソフトウェアライフサイクル全体で</u>セキュアなソフトウェアを開発するための<u>フレームワーク</u>（Secure Software Development Framework：SSDF）。• 2022年発行。
OMB M-22-18 （M-23-16に更新）	<ul style="list-style-type: none">• 政府機関が、ソフトウェアベンダーに対して、<u>SSDFの実装の適合性を証明する自己適合宣言書</u>の取得を要求することを定める文書。自己適合宣言書では、SP800-218から抽出した最低限とするセキュアなソフトウェア開発プラクティスに従っていることを宣言。• 2023年発行。
Supply Chain Cybersecurity Principles	<ul style="list-style-type: none">• 米国のエネルギー事業者とそのサプライヤー向けのサプライチェーン・サイバーセキュリティ原則。• 2024年公表。
Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default	<ul style="list-style-type: none">• ソフトウェア開発事業者が脆弱なソフトウェアを商品化しないよう、そして<u>顧客にセキュリティ確保の負担をできるだけ負わせない</u>ようにすることを目指し、<u>セキュア・バイ・デザイン／デフォルトの概念</u>に基づき、ソフトウェア開発事業者に求められる3つの原則を整理。• 2023年発行。内閣サイバーセキュリティセンターとJPCERTも署名。

経済産業省 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：資料3：P09,10,11

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/cyber_infrastructure/002.html

TLP: CLEAR

ソフトウェアサプライチェーンに関わる諸外国の取組（つづき）

その他

日米豪印サイバーセキュリティ・パートナーシップ：共同原則

- 政府間及び産業界のパートナーとの間で脅威情報を迅速かつ時宜を得た形で共有すること、政府が調達するソフトウェアに対して最低限のソフトウェアセキュリティ標準を実施すること等を求める。
- 2022年公表。

ソフトウェア・セキュリティに関する日米豪印共同原則

- 政府のためのソフトウェアの開発、調達及び利用の指針となる最低限のサイバーセキュリティ・ガイドライン。
- 2023年公表。

国内でも諸外国と同等の取組を行う事になってきました。
経済産業省が主体となって動いているようです。

経済産業省の「サイバー・フィジカル・セキュリティ確保に向けたソフトウェアの管理手法等検討タスクフォース」にて話が進められています。

- 「サイバーインフラ事業者に求められる役割の検討会」
 - 第二回まで実施され、政府調達等で話を進めている
 - 現状、自己認証/第三者認証で調達時の評価に加える方針のようだ
 - サプライチェーン対策を進めるため、自己認証/第三者認証により補助金を出す方向のようだ



経済産業省 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：資料3：P09,10,11

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/cyber_infrastructure/002.html

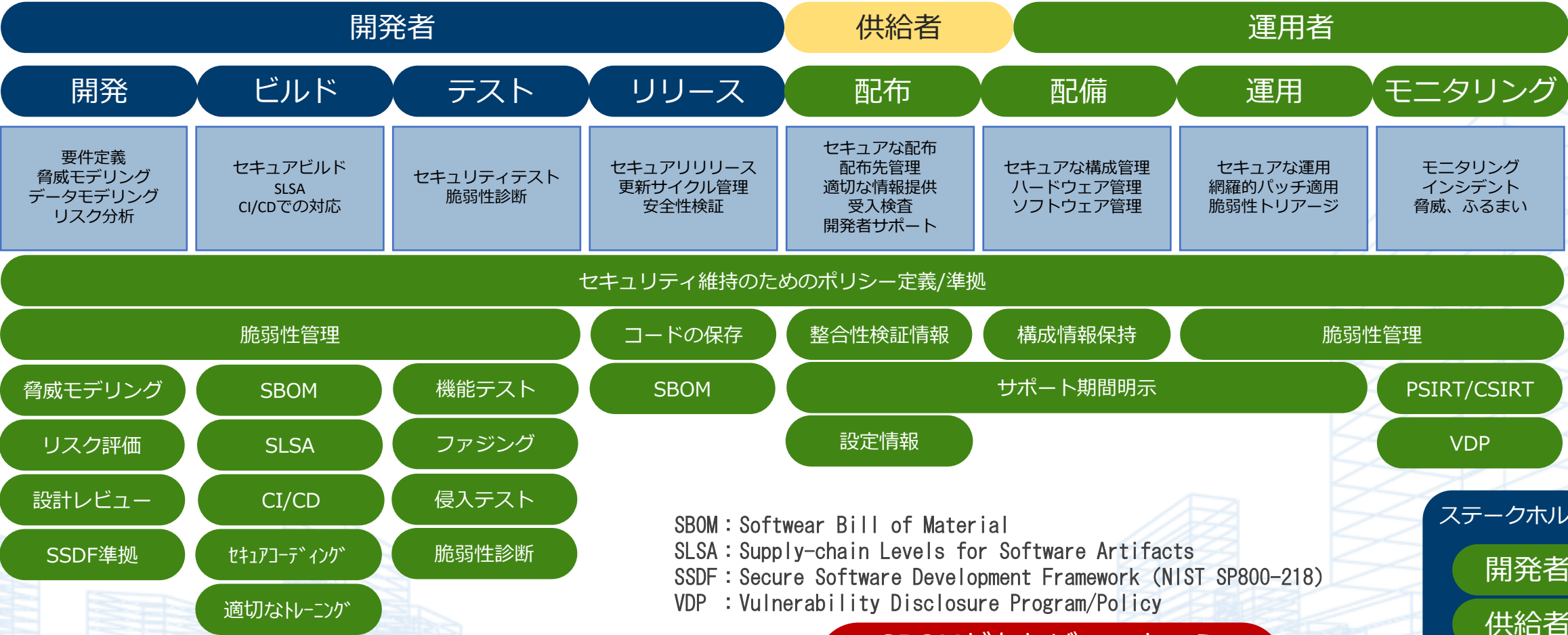
03 現在想定されている方法論

全体として、以下が求められることとなっています。

要求事項の概要

- 要求事項はカテゴリとして整理する。複数の個別要求（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		要求事項
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：経営層のコミットメントと人員の整備 (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 顧客の経営層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 顧客の経営層のリーダーシップによるリスク管理 (6)-2 顧客の経営層のリーダーシップによるソフトウェアの調達、運用



おおよそまとめると上記のようになります。

- 本来はステークホルダーごとに定義されているが、混在して記載/完全性はない

SBOMがあればいいという
単純な話ではない

全体として、既存では個別に実施していたものを、サプライチェーン全体として取り扱うこととなります。

Japan SBOM Summitなどでの話を総合すると、経済産業省は以下の方針と推察されます。

- できるだけ、法的拘束/罰則を設けずに、事業者自身の取組で達成されるようにしたい
 - SBOMのように、具体的な手法/手引きを用意することで普及を目指す
 - 自己認証制度の取組は他国でも検討されており、補助金等のメリットにより普及を目指すと思われる
- 政府調達案件で必須化されると思われる
 - 直接の入札要件とはされずとも、達成状況が加点要素となりえる
- とはいえ、タイムラインはあまり見えていない
 - 現在議論中の為、か。



04 まとめ

他国を含め、サプライチェーンセキュリティ対策は必須な状況となっています。

今の時点ではすぐに必須になるとは考えられませんが、数年後には徐々に対応が必要になると考えられます。対応しないと入札等で不利になる可能性が高いです。

まずは、出来る部分から対応していくのが良いと考えられます。

- SBOM、脅威モデリング、セキュアコーディング、CI/CDの活用、脆弱性検査や脆弱性管理、などの今までの延長線上のものを進める
- VDP、SSDF（NIST SP800-218）辺りはもう少し資料が出てくれば、そこから対応していく
- SLSAなどは、まだ発展途上に見えるので、ある程度普及してから対応で良さそう

今後の国としての動向も追っていく必要があります。

SBOMやVDPなどの個別の話は
今回は時間がないので割愛しました





Appendix

- 経済産業省
 - サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース
 - https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/index.html
 - サイバーインフラ事業者に求められる役割等の検討会
 - 第1回
 - https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/cyber_infrastructure/001.html
 - 第2回
 - https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/cyber_infrastructure/002.html
 - サイバー攻撃への備えを！「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改定手引きを策定しました
 - <https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html>
 - 「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめました
 - <https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html>
- SLSA (Supply-chain Levels for Software Artifacts)
 - <https://slsa.dev/>
- 米国
 - NIST SP 800-218 Secure Software Development Framework (SSDF)
 - <https://csrc.nist.gov/pubs/sp/800/218/final>
 - OMB M-22-18 -> M-23-16
 - <https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf>
 - Securing the software supply chain: recommended practices guide for suppliers and accompanying fact sheet
 - <https://www.cisa.gov/resources-tools/resources/securing-software-supply-chain-recommended-practices-guide-suppliers-and>
 - Shifting the balance of cybersecurity risk: security-by-design and default principles
 - <https://www.cisa.gov/news-events/alerts/2023/04/13/shifting-balance-cybersecurity-risk-security-design-and-default-principles>
- 英国
 - Code of Practice for Software Vendors: callfor views
 - <https://www.gov.uk/government/calls-for-evidence/call-for-views-on-the-code-of-practice-for-software-vendors>
 - Guidelines for secure AI system development
 - <https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf>

リスク評価手法としては、おおよそ以下のようなものがあります。

- 一般論として

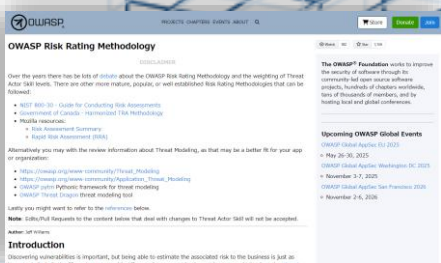
➤ **リスク** = **脆弱性** × **発生可能性** × **影響**

- ✓ **脆弱性** : 脆弱性それ自体の影響 (CVSS Score等)
- ✓ **発生可能性** : 脆弱性を使われる可能性 (KEVC、EPSS、構成等)
- ✓ **影響** : システムの価値 (保有データ等)

- OWASP Risk Rating Methodology (OWASPリスク格付け手法)

➤ **リスク** = **可能性** × **インパクト** (Informal Methodでの言及)

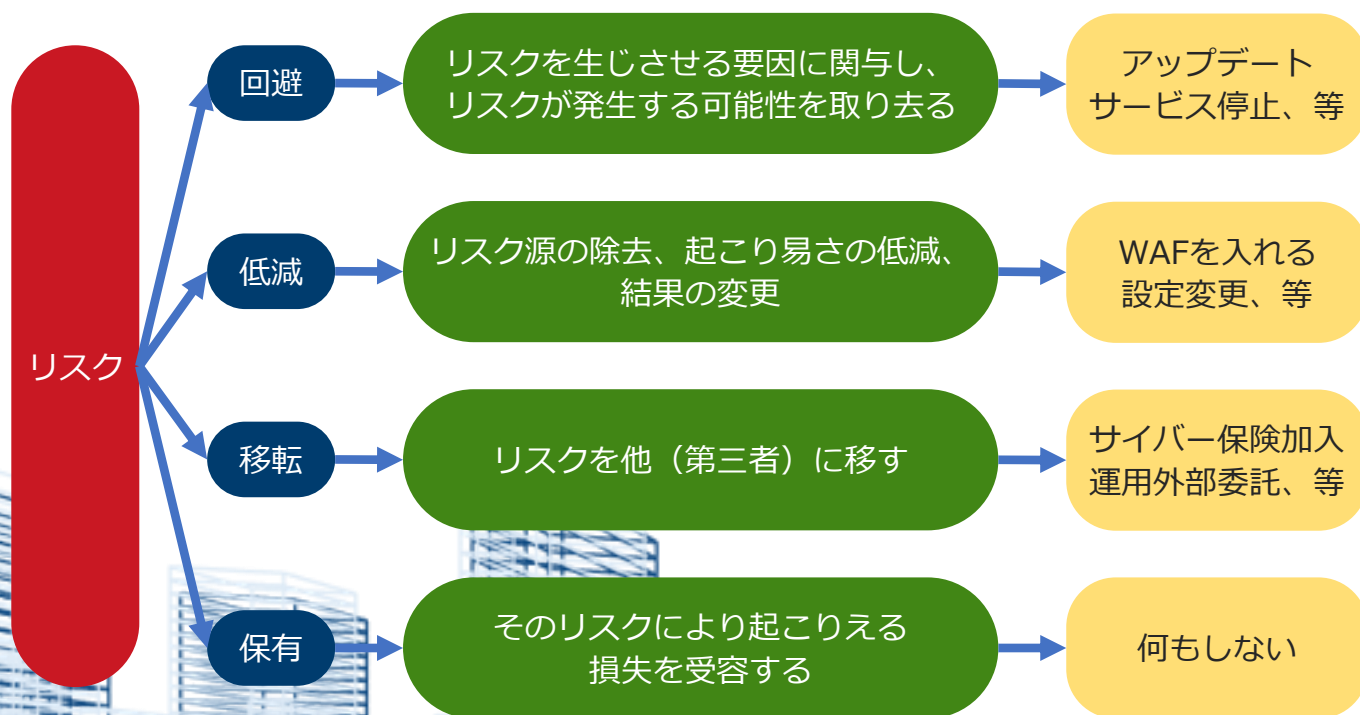
- ✓ **可能性** : 脅威の要因、脆弱性の要因
- ✓ **インパクト** : 技術的な影響、ビジネスへの影響



OWASP : Risk Rating Methodology
https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

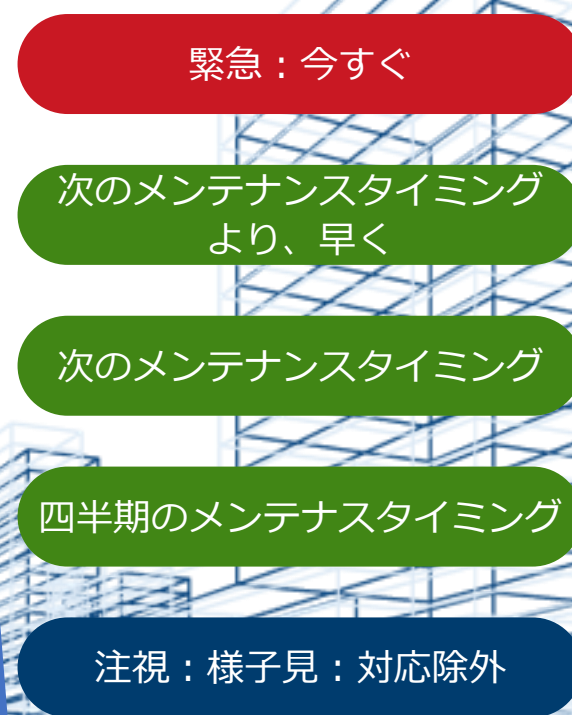
脅威の要因	スキルレベル	動機	機会	サイズ
脆弱性の要因	検出の容易さ	悪用の容易さ	認識	侵入検知
技術的な影響	機密性の喪失	整合性の喪失	可用性の喪失	説明責任の喪失
ビジネスへの影響	金銭的損害	評判の低下	コンプライアンス違反	プライバシー侵害

また、今までは「アップデートを行うか/否か」で判断でしたが、近年は**リスクに対する対応**という観点で対応方法を検討し、対応方法と期日を組み合わせています。



図：リスクと取り得る対応

対応速度



図：脆弱性への対応速度



※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。

※ LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。その他記載されている会社名、製品名は一般に各社の商標または登録商標です。