※本資料は予告なく変更される場合があります。

仮訳

サイバーセキュリティリスクのバランスを変える:

セキュアバイデザイン、セキュアバイデフォルトの原則とアプローチ

発行:2023年10月16日

サイバーセキュリティ・インフラ安全庁（CISA）

CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL
NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas

目次

設計から弱い状況(概要) 3

What’ s New 4

この文書の使用方法 5

セキュアバイデザイン 6

セキュアバイデフォルト 6

ソフトウェア作成業者向けの提言 7

ソフトウェア製品のセキュリティ原則 7

原則１：顧客にもたらされるセキュリティの結果に責任を負う 8

説明 8

この原則の実例 11

原則２：徹底的な透明性と説明責任を果たす 15

説明 15

この原則の実例 16

原則３：トップ主導 18

説明 18

この原則の実例 18

セキュアバイデザインの手法 19

セキュアバイデフォルトの手法 21

セキュリティ強化ガイドとセキュリティ緩和ガイド 23

顧客への提言 23

免責 24

資料 24

参考資料 26

変更履歴

版	日付	修正/変更内容	影響のある頁/節
1.0	*2023 年 4 月*	初版	
2.0	*2023 年 10 月*	5 頁の「What’ s New」を参照 *３つの基本原則の説明と例*	全体を通じて更新

設計から弱い状況(概要)

技術は、我々の日常生活のほぼすべての面に溶け込んでいる。身分証明書管理から医療に至るまで、我々の経済や生活、健康にも直接的に影響を与えうる重要システムが、益々インターネットに直結するシステムに接続するようになっている。このような利便性の欠点の一例として、病院が手術を中止し、治療をたらい回しなってしまうようなグローバルなサイバー攻撃の被害が挙げられる。安全でない技術や重要システムの脆弱性は、悪意あるサイバーの被害を招き、潜在的な安全上[1]のリスクに繋がる。

結果として、ソフトウェア作成業者がセキュアバイデザインとセキュアバイデフォルトを製品の設計と開発段階から重視することがかつてないほど重要になっている。ソフトウェアの品質保証に関して業界が前進するよう尽力するベンダーもあるが、引き続き遅々として進まないままのベンダーもいる。本文書を執筆・作成した組織（これ以降は「署名組織」）は、全ての技術製造業者に対し、顧客が自身のシステムに対するサイバー攻撃を緩和すべく、常に監視、日常的なアップデートおよびダメージコントロールを行わないで済むことを含め、顧客に係るサイバーセキュリティの負担を軽減することをベースに製品を作るよう強く推奨する。また、ソフトウェア作成業者には、設定、監視、定期的なアップデートの自動化を容易にするような方法で製品を作成するよう促したい。作成業者は、自身の顧客のセキュリティの結果を改善することに責任を持つことが望まれる。歴史を見ると、ソフトウェア作成業者は、顧客が製品を使用した後に脆弱性を発見し、修正することに頼り、顧客に対しては自己負担でこれらのパッチを適用させることを強いてきた。セキュアバイデザインの実践を取り入れることによってのみ、このような頻繁に修正パッチを作成して適用するという悪循環を断つことができる。注釈：「セキュアバイデザイン」という用語は、セキュアバイデザインとセキュアバイデフォルトの双方を包含する。

署名組織は作成業者に対し、この高いソフトウェアセキュリティの水準を達成するために、性能や製品の市場投入の早さよりも、製品セキュリティを重要な必須要件として取り込むことを最優先にするよう推奨する。エンジニアリングチームは、時間が経つにつれ、セキュリティが真に設計に取り入れられ、簡単にその維持ができる、通常のリズムを新たに確立できるであろう。この観点から、欧州連合は、Cyber Resilience Act において製品セキュリティの重要性を補強し、作成業者が脆弱な製品を商品化しないよう、製品のライフサイクル全体を通じたセキュリティを実装するのが望ましいことを強調している。

署名組織は、技術とその技術に関連する製品が顧客にとって一層安全である未来を創造するために、作成業者に対して設計・開発プログラムを見直し、セキュアバイデザインとセキュアバイデフォルトの製品のみ出荷を許可するよう促したい。セキュアバイデザインの製品とは、顧客の安全が中核

となるビジネス目標として開発のはるか前から概念付けられ、技術上の性能に留まらないものを言う。セキュアバイデザインの製品は、開発開始前にその目標から開始する。既存の製品は、複数の段階を経て、セキュアバイデザインの状態に進化することができる。また、セキュアバイデフォルトの製品とは、設定変更をする必要がほとんどなく、追加コストなしでセキュリティ機能が備わっているもので、「購入後すぐ（out of the box）」に安全に使用できるものを言う。これら2つの理念は、共に、安全を維持する負担の多くを作成業者に移し、顧客にとっては、設定ミスや迅速ではないパッチの適用などを起因としたインシデントの被害を受ける可能性を減らすことができる。

サイバーセキュリティ・インフラ安全庁（CISA）、国家安全保障局（NSA）、連邦捜査局（FBI）、並びに次の国際パートナーは、この指針において、ソフトウェア作成業者が製品の安全を確保するロードマップとなる提言を行う。

- 豪州サイバーセキュリティセンター（ACSC）
- カナダサイバーセキュリティセンター（CCCS）
- 英国国家サイバーセキュリティセンター（NCSC-UK）
- ドイツ連邦情報セキュリティ庁（BSI）
- オランダ国家サイバーセキュリティセンター（NCSC-NL）
- ノルウェー国家サイバーセキュリティセンター（NCSC-NO）
- ニュージーランドコンピュータ緊急対応チーム（CERT-NZ）およびニュージーランド 国家サイバーセキュリティセンター（NCSC-NZ）
- 韓国インターネット振興院（KISA）
- イスラエル国家サイバー総局 （INCD）
- 日本内閣サイバーセキュリティセンター（NISC）およびJPCERTコーディネーションセンター（JPCERT/CC）
- 米州・政府サイバーインシデント対応チーム（CSIRT）OAS/CICTEネットワーク
- シンガポールサイバーセキュリティ庁（CSA）
- チェコ国家サイバー情報セキュリティ庁（NÚKIB）

署名組織は、多くの民間パートナー企業がセキュアバイデザインとセキュアバイデフォルトを前進させるべく貢献していることを認識している。この指針は、技術が設計段階および初期設定から安心、安全かつ強靭さを備えた未来を実現するため、必要な優先順位、投資、意思決定についての国際的な対話を促すことを意図している。署名組織は、こうした目標達成のために、関心のある方々からこの指針に対するフィードバックを求め、さらなる指針の改善、明確化および発展のためにヒアリングセッションを設けたいと考えている。

製品の安全性の重要性については、CISAの論文「The Cost of Unsafe Technology and What We Can Do About It」を参照ありたい。

What’s New

本報告の初版は、ソフトウェア業界内で多くの対話を生み出した。組織や個人が被害を受けていると

いうような毎日流れるニュースは、ソフトウェア製品における慢性的かつ体系的な問題に対処する方法についてより多くの会話を交わす必要性を強調している。

2023年4月の第1版発表後、署名組織は何百もの個人、企業、業界団体から思慮に富むフィードバックを受け取った。フィードバックの中で最も多かった要望は、3つの原則について、より詳しく説明してほしいというものであった。これらの原則は、作成業者とその顧客の双方に適用されるからである。本文書では、元々の報告を発展させ、作成業者や顧客の規模、顧客の成熟度、原則の適用範囲など、その他のテーマについても触れている。

ソフトウェアはあらゆるところに存在するが、ソフトウェアシステム、ソフトウェア製品の開発、顧客への展開と維持管理、他のシステムとの統合といった全ての範囲を十分にカバーすることのできる報告は１つもない。以下の指摘のうち特定の環境に明確に位置づけることができないものについては、この文書で示された助言をどのように特定のセキュリティ上の改善に繋げるか、コミュニティからの意見をお待ちしている。

この報告は、人工知能（AI）ソフトウェアシステムやAIモデルの作成者にも適用される。AIシステムやAIモデルは従来のソフトウェアとは異なるかもしれないが、根本的なセキュリティ上の実践はそれらにも適用される。いくつかのセキュアバイデザインの実践は、AI特有の考慮を説明するため修正される必要があるが、3つの包括的なセキュアバイデザイン原則は全てのAIシステムに適用される。

セキュアバイデザイン原則に一致するようソフトウェア開発ライフサイクル（SDLC）を変革することは簡単ではなく、時間もかかることを認識している。さらに、小規模のソフトウェア作成業者は、これら指摘の多くを実施するのに苦労するかもしれない。我々は、ソフトウェア業界が、製品を安全にするツールと手順を広く入手できるようにさせる必要があると考えている。人々や組織がソフトウェアのセキュリティ改善に集中すればするほど、イノベーションの余地が生まれ、大小のソフトウェア作成業者のギャップを狭め、全ての顧客が裨益すると信じている。

元々のセキュアバイデザイン報告に対する、この補足ガイダンスは、技術エコシステムを支える、多くの相互依存関係にあるステークホルダーコミュニティとの関係を構築するという、我々のコミットメントの一部を成す。これはエコシステムの多くの構成員からのフィードバックの結果であり、我々はさまざまな視点からの意見に耳を傾け、学んでいくことを続ける。この先、多くの課題が待ち受けているが、セキュアバイデザインの理念を既に採用し成功している人々や組織を学ぶにつれ、我々は信じられないほど楽観的になっている。

この文書の使用方法

我々は、ソフトウェア作成業者がこの文書の原則を支持するよう促したい。ソフトウェア作成業者は、以下に列挙された段階に沿って実行した行動を公に文書化することで、そのコミットメントを示すことができる。我々は、ソフトウェア作成業者にこの原則の精神に合致する戦術を見いだし、セキュアバイデザインの理念を体現していることを、懐疑的な現在および潜在的な顧客にも説得力のある形で説明できるように成果物を作ることを奨励する。

作成業者が取るべき行動に加え、顧客もこの文書を活用することができる。ソフトウェアを購入する企業は、この文書に記載されている原則を遵守している事例から着想を得ながら、ベンダーに厳しい質問をすることが適当である。そうすることで、顧客は、製品がよりセキュアバイデザインとなる方向に市場をシフトさせることを支援できる。顧客がベンダーに尋ねることができる質問の例は、CISA の「CISA’s Guidance for K-12 Technology Acquisitions」に示されている。

我々は、企業の顧客が、調達プロセス、ベンダーのデュー・デリジェンス評価、企業のリスク受容の

CISA | NSA | FBI | ACSC |CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL
NCSC-NO | NÚKIB | INCD | KISA |NISC-JP | JPCERT/CC | CSA | CSIRTAmericas

決定、およびベンダーを評価する際のその他のステップに、これらの慣行を組み込むことを奨励する。また、顧客は、各ベンダーがセキュアバイデザインを実践していることを文書化するよう、ベンダーに働きかけることが望ましい。これらをあわせて、セキュリティを強く要求するシグナルを生み出し、作成業者がよりセキュリティを高めるための措置を講じることを奨励し、可能にすることができる。言い換えれば、セキュアバイデザインの哲学をソフトウェア作成業者に浸透させるのと同様に、顧客とともに「セキュアバイデマンド」の文化を創造する必要がある。

セキュアバイデザイン

「セキュアバイデザイン」とは、技術製品が、悪意あるアクターによって端末機器、データ、インフラに不正にアクセスできないよう合理的に保護されている形で作られることを意味する。ソフトウェア作成業者はリスク評価を行い、重要システムへの主なサイバー脅威を特定し、洗い出し、その上で、製品設計にあたり現下のサイバー脅威状況を考慮した防護を講じることが適当である。

悪意あるアクターがシステムに侵入し、機微データに不正アクセスされないよう、安全な IT 開発の実践と何層にも防御する「深層防御(defense-in-depth)」が推奨される。署名組織は、さらに作成業者に対し、システムに対する全ての脅威に対処し、システムの展開プロセスの各段階で対応できるよう、製品の開発段階から自己に適合させた脅威モデルを利用することを推奨する。

署名組織は、作成業者に対し、製品やプラットフォームに包括的な安全措置を講じることを求める。セキュアバイデザインの開発のためには、ソフトウェア作成業者は、後から「追加（bolted on）」できない製品設計や開発プロセスにおける各層において、固有のリソースを戦略的に投資する必要がある。また、セキュアバイデザイン開発は、セキュリティを単なる技術上の特性ではなく経営の優先事項とする、ソフトウェア作成業者のトップ経営層による強いリーダーシップが不可欠である。この経営陣と技術チームとの連携は最初の設計・開発段階から、顧客への展開や維持管理まで及ぶ。ソフトウェア作成業者は、安全を重視し、難しいトレードオフに対応し、顧客にとって見えにくい対策（例えば、脆弱性を取り除いたプログラミング言語への移行など）にも投資することが求められる。魅力があるが攻撃面を増加させてしまう機能ではなく、顧客を守る機能、メカニズム、ツール実装を優先することが望ましい。

悪意ある攻撃者が技術の脆弱性を悪用するという脅威を終わらせる単一の解決方法は存在せず、セキュアバイデザインの製品から脆弱性が無くなることもないであろう。しかしながら、脆弱性の多くは、比較的限られた根本原因に起因する。作成業者は、既存の製品をセキュアバイデザインの慣習に沿わせるための書面のロードマップを作成し、例外的な状況でのみ逸脱が許されることとするのが望ましい。

署名組織は、作成業者が顧客のセキュリティの責任を引き受け、顧客のセキュリティを保障すると開発コストが上昇することを認識している。しかし、革新的な技術製品を開発し、既存の製品を維持しながらセキュアバイデザインの実践に投資することで、顧客の安全は大いに改善され、被害の可能性は低くなる。すなわち、セキュアバイデザインの原則は、顧客の安全とブランド評価を高めるだけではなく、その実践が長期的には製品の維持とパッチ適用のコストを低減することができる。

ソフトウェア作成業者向けの提言の項では、製品開発に係る行動や政策を一覧にした。

セキュアバイデフォルト

「セキュアバイデフォルト」とは、製品が、追加費用なく、購入後すぐ（out of the box）でも、普及

している攻撃技術に対して強靭な状態にあるものを言う。これらの製品は、エンドユーザーが追加的な措置を講じる必要なく、最も普及した脅威や脆弱性から自身を保護することができる。また、セキュアバイデフォルトの製品とは、安全な初期設定から逸脱した場合には、追加措置を講じなければ被害される可能性が高まることを顧客にきちんと把握させるよう設計されているものを言う。セキュアバイデフォルトは、セキュアバイデザインの一形態である。

- 安全な設定が初期設定の基準となることが適当である。セキュアバイデフォルトの製品とは、悪意あるサイバー攻撃者からの防御に必要な最も重要となるセキュリティ制御を自動的に有効化し、追加費用なく追加のセキュリティ制御ができるものである。
- セキュリティ設定の複雑さを顧客側の問題とするのは適当でない。顧客組織の IT スタッフは、しばしばセキュリティと運用上の責任の双方を負うこととなり、結果として、セキュリティ上の意味合いや、確かなサイバーセキュリティ態勢が求められるような対応策の理解や対処に十分時間がとれなくなっている。作成業者は、自社製品が「セキュアバイデフォルト」水準に従い、安全に作成・配布・利用されことを保証するために、安全な製品設定を行うこと、すなわち、「初期設定」を安全にすることで、顧客を支援することができる。

「セキュアバイデフォルト」の製品の作成業者は、追加のセキュリティ設定を実装するために追加料金を求めない。このセキュリティ設定は、すべての新車にシートベルトが付いているように、標準製品に備わっている。セキュリティは贅沢なオプションではなく、全ての顧客が作成業者に交渉や追加的な支払いをすることなく期待できる標準装備に近いものであることが望ましい。

> *セキュリティは贅沢なオプションではなく、全ての顧客が作成業者に交渉や追加的な支払いをすることなく期待できる標準装備に近いものであることが望ましい。*

ソフトウェア作成業者向けの提言

この共同指針は、ソフトウェア作成業者に対し、IT セキュリティを実装・確保するための書面でのロードマップを作成するに当たっての提言を行う。署名組織は、ソフトウェア作成業者に対し、セキュアバイデザインとセキュアバイデフォルトの原則を通して、主体的に顧客のセキュリティ確保に取り組み、下記の項で概略する戦略を実行するよう提言する。

ソフトウェア製品のセキュリティ原則

ソフトウェア作成業者は、ソフトウェアセキュリティを優先するような戦略目標を設定することが望ましい。署名組織は、ソフトウェア作成業者が製品開発・設定・搬送する前の設計プロセスにソフトウェアセキュリティを組み込むうえでの指針となる以下の 3 つの中核となる原則を策定した。

1. **顧客にもたらされるセキュリティの結果に責任を負い**、そのため製品を発展させる。セキュリティの負担は顧客だけが負うのは望ましくない。
2. **徹底的な透明性と説明責任を受け入れる。**ソフトウェア作成業者は、安全で安心な製品を販売することに誇りを持ち、そのようにできることでソフトウェア作成業者コミュニティにおける他の

作成業者とは差別化することが適当である。これには、初期設定における強い認証メカニズムの採用など、顧客の利用から得られた情報の共有が含まれる。また、脆弱性に関するアドバイザリーの発行やこれに関連する共通脆弱性識別子 （CVE）の登録の完全性および正確性を確実にするという力強いコミットメントも含まれる。ただし、CVE の数は健全なコード分析・試験を行っている証左であり、マイナスの指標と評価しないよう注意して頂きたい。

3. **これら目標達成のため企業の組織構造および経営層を構築する。**製品の安全には専門知識が重要であるが、組織の変革を実行するのは経営層の主要な意思決定者である。ソフトウェア作成業者が製品開発の重要な要素としてセキュリティを優先させるという経営者層のコミットメントを得るには、顧客とのパートナーシップ構築が不可欠である。

作成業者は、これらの 3 つの原則を実現するため、幾つかのオペレーション上の手法を考慮して開発プロセスを進めるのが望ましい。

例えば、組織内におけるセキュアバイデザインとセキュアバイデフォルトの重要性に関する理解推進をするための、経営層との定期会議を開催する。これらの原則に従って製品を開発したチームに報酬を与える社内ポリシーや手続を策定するのが望ましい。これには、優れたソフトウェアセキュリティの実践に対する表彰や、職種ごとの階級設定や昇進要件におけるインセンティブ付けが含まれる。

ビジネスの成功のために企業活動の中心にソフトウェアセキュリティの重要性を据えることもできるだろう。例えば、ソフトウェアセキュリティ基準と説明責任を直接結び付け、ビジネスと IT 活動を同時に支える「ソフトウェアセキュリティリーダー」や「ソフトウェアセキュリティチーム」の任命を検討する。また、ソフトウェア作成業者は、頑強かつ独立した製品セキュリティ評価プログラムを確保することが望ましい。

人員割当および開発時に、カスタマイズした脅威モデルを使用し、最も重要あるいは影響の大きい機能を優先化させる。脅威モデルを使用することで、製品の特定のユースケースを考慮や、開発チームが製品の強化をすることができる。最後に、経営層幹部は、製品の優位性や質を判断する材料として安全な製品を実現する説明責任を開発チームに負わせることが望ましい。

2023 年 10 月の本ガイダンスの更新の一環として、これらの 3 つの原則は、次のとおり、説明、実例、証拠を詳述する。

原則 1 ：顧客にもたらされるセキュリティの結果に責任を負う

説明

今日のベストプラクティスは、作成業者に対し、アプリケーションの堅牢化、アプリケーションのセキュリティ機能、アプリケーションの初期設定など、製品のセキュリティ対策に投資することを求めている。

ソフトウェア作成業者は、アプリケーションを侵害したい悪意のあるアクターのコストを上げるためのプロセスと技術を用いて**「アプリケーションの堅牢化」**を実施する必要がある。アプリケーションの堅牢化のプロトコルと手順は、知識のある悪意のあるアクターによる攻撃から製品を抗することに役立つ。堅牢化、製品セキュリティ、強靭さといった用語は、全て製品品質に密接に関連している。この考え方は、セキュリティとは「追加される」ものではなく、「織り込んである」ものであるというものである[1]。セキュリティを織り込むことで、ソフトウェア作成業者は顧客のセキュリティを強化するだけでなく、製品品質を高めることもできる。こうした戦術としては、ユーザーの入力が検証されサニタイ

ズされ、コードに直接入力されないようにすること（例えば、代わりにパラメータ化したクエリを利用する）、メモリに安全なプログラミング言語を使用すること、厳格なソフトウェア開発ライフサイクル（SDLC）管理を行うこと、ハードウェアに裏打ちされた暗号鍵管理を使用すること、などが含まれる。

アプリケーションはサイバーセキュリティに関する**アプリケーション機能**をサポートする必要がある。「性能」と呼ばれることがあるこれらの機能は、顧客のセキュリティ態勢の維持や向上を支援するよう、製品・サービスの性能を拡張する。セキュリティ関連の機能の例には、すべてのネットワーク接続に対するトランスポート層セキュリティ(TLS)のサポート、シングルサインオン(SSO)のサポート、多要素認証(MFA)のサポート、セキュリティイベント監査ログ、役割ベースのアクセス制御(RBAC)、および属性ベースのアクセス制御(ABAC)が含まれる。

これらの製品の機能の中には、顧客が既存の環境やワークフローに製品を容易に統合できるように設定可能なものもある。それらの構成が意味するのは、アプリケーションは、顧客が構成するまでに**初期設定**を持たなければならないということである。これらの初期設定は、顧客が大量の技術製品を安全にするために費やすリソースを少なくできるように、「箱から出してすぐに」安全に設定されている必要がある。

アプリケーションの堅牢化、アプリケーションセキュリティ機能、アプリケーションの初期設定といった各要素は、アプリケーションのセキュリティや、その結果としての顧客のセキュリティ態勢に役割を果たす。作成業者は、これら各要素や、互いの関連性を考慮するのが望ましい。作成業者は、これら要素を製品に組み込む投資以上のことを考えることが望ましい。作成業者は、さらに一歩踏み込んで、これら要素が顧客の実際のセキュリティ態勢を如何に変化させるか（良い方向でも、悪い方向でも）についても考慮することが望ましい。

作成業者は、自社の努力や投資だけで評価するのではなく、顧客にもたらされるセキュリティの結果に対して責任を負うことが望ましい。その責任は、被害の可能性を最も低く抑えることができる作成業者と共に上流部門が負うことが望ましい。

現在は残念ながらそうなっていない。あまりにも多くの作成業者が、セキュリティの責任を顧客に転嫁し、包括的に**アプリケーションの堅牢化**を行う投資を行っていない。例えば、作成業者がある脆弱性にパッチを適用しても、すぐに同様の脆弱性が明らかになることがある。これは、根本原因に対処せず、対処療法的に対処するのみだからである。製品は、同じ属性の脆弱性であっても、コードベースのさまざまな部分で異なる緩和策を実施しているかもしれない。例えば、作成業者がある入力をサニタイズする箇所の脆弱性を修正した後、研究者や攻撃者が、改善されたサニタイズを回避するコードパスを発見した事例がある。作成業者は、コードベースを統一してアプリケーション全体にわたり脆弱性全体を除去するのではなく、一度に一つずつ脆弱性の修正を適用したのである。

アプリケーションの機能とは、顧客にメリットとリスクを生み得る。多くの外部システムやバージョンとの連結を可能にする機能は、製品の価値を大きく高めることができる。しかし、ネットワークプロトコルのように利用廃止までの計画がないような支援機能は、その機能を使い続ける意味を十分に理解していない場合には顧客をリスクに晒す可能性がある。例えば、製品の中には、1990 年代や 2000 年代に起源を持ち、現在では安全でないことが知られているネットワークプロトコルを使い続けているものがある。もちろん、顧客が最新のセキュリティ対策をアップグレードし展開することを遅らせてしまう要因は多くある。使用している製品が組織のネットワークに統合されていて最新のセキュリティ対策ができないが故に IT チームが最新の状態になれない場合がある。しかし、ソフトウェア作成業者は、これらのパターンを計画プロセスの中で考慮し、顧客が最新状態となるよう奨励できる。

アプリケーションの初期設定も、顧客にとって潜在的なリスクとなり得る追加的な領域である。作成業者は特定の機能をデフォルトで有効にし、顧客が望むアプリケーション機能を使いやすくすることが良くある。しかし、これらの機能やプロトコルを必要としない顧客にとっては攻撃面を拡大するだけである。さらに、多くのセキュリティ制御はデフォルトで無効に設定されているか、顧客側がセキュリテ

ィを高めるために時間をかけて設定を行う必要がある。明示的な脅威モデルを作ることは、どの機能をデフォルトで有効化するか、または、どの設定がセキュアバイデフォルトに必要なのかを決定するのに役立つ戦術である。別の戦術としては、管理者にとって分かりやすい機能とする方法を調査することが挙げられる。

作成業者の中には、一部あるいは全ての顧客にリスクを生じさせる可能性がある初期状態で製品を出荷している者もいる。こうした作成業者は、より安全な初期設定をするのではなく、顧客が自費で実装しなければならない「**セキュリティ強化ガイド**」を作成することが多い。セキュリティ強化ガイドには、いくつかの問題がある。セキュリティ強化ガイドの中には見つけるのが難しく、十分にサポートされていないものがある。また、実装が複雑なものや、拡張モジュールを書くためにソフトウェア開発を必要とするものさえある。その他、さまざまな設定が攻撃面を変化させることを十分理解できる程にサイバーセキュリティに関する豊富な経験を持っていることを前提としているものもある。攻撃側を十分理解しない実務者は、セキュリティ強化ガイドの指示を然るべく実装できない可能性がある。指示がトレードオフを明確にしていない場合は特にそうである。さらに、すべてのセキュリティ強化ガイドが攻撃者の手法や経済状態に精通したエンジニアによって書かれているわけではないため、忠実に実装しても効果のない場合もある。何百万もの顧客が、多くの場合リソースに制約のある環境において、ソフトウェアまたはシステムの複数のインスタンスを強化する責任を負っていることを念頭に置く必要がある。これでは単純に機能しない。

アプリケーションは、その設定がデフォルトであろうと、顧客が設定したものであろうと、脅威状況に対する作成業者の最新の理解に照らして継続的に評価する必要がある。アプリケーションは、それらの設定から生じる潜在的なリスクについての明確な指標があることが望ましく、それらの指標は公開されるのが望ましい。最新の自動車がシートベルトに関する指標があり、シートベルトを締めずに運転しようとするとこうした指標が表示されるのと同じように、ソフトウェアはシステムのセキュリティ状態についての指標を明確に表示することが望ましい。もし、あるアプリケーションが管理者アカウントに多要素認証（MFA）を要求しないように設定されている場合、管理者に MFA 設定をしないと自分自身と組織全体が危険にさらされていることを定期的に知らせなければならない。加えて、もしアプリケーションが、脆弱な暗号が実装されていると今日では知られているような古いプロトコルをサポートするよう設定されている場合、組織が危険にさらされていることを管理者に定期的に明らかにし、その状況を解消するためのリソースを組織が提供する必要がある。我々は、管理者にセキュリティガイドを解釈してもらうための時間、専門知識および認識を要求することに依存するのではなく、作成業者に対して、製品に定期的な通知を出すよう組み込んで実装することを強く求める。セキュリティと利便性への配慮をバランスさせたイノベーションを実現する機会は明らかに存在する。

上記の各要素は、顧客が被害の可能性を減らすために、追加の**セキュリティ製品について**調査し、資金を拠出し、購入し、人員を配置し、導入し、監視する必要があるという容認し難い状況を作り出す。中小規模の組織（SMO）では、こうしたことができないことが一般的である。専門知識、資金、時間が不足しており、それが新しいことをする余力と機能性に負担をかけ、セキュリティの優先順位を低くせざるを得ず、これらが合わさることで集合的なリスクが増大する。逆に、セキュリティ投資は比較的少数の作成業者でしか有効とはならない。この問題を要約する常套句は、「ソフトウェア業界はより多くの安全な製品が必要なのであって、より多くのセキュリティ製品が必要なのではない」というものだ。ソフトウェア作成業者はその変革をリードするのが望ましい。

> *ソフトウェア業界はより多くの安全な製品が必要なのであって、より多くのセキュリティ製品が必要なのではない。作成業者はその変革をリードするのが望ましい。*

今日、我々は、特定のセキュリティ機能を有効にしなかったり、特定の強化ガイダンスに従わなかったりしたために、顧客が被害を受けたと説明する作成業者のコメントを読むことがある。その代わりに、被害を受けた後、作成業者は特定のセキュリティ機能または特定の強化ガイドがあればその被害を防げたかどうかを説明し、追加費用無しでそれをデフォルトにすることを検討することが望ましい。製品自体の設計・実装局面での強化が十分でなかった場合、作成業者は、製品ラインから同種の脆弱性を排除するためにどのように取り組んでいるかを説明することが望ましい。

ソフトウェア作成業者には、自社製品がセキュリティを最優先して設計・開発されていることを保証する責任がある。そのためには、自らの努力の**成果を客観的に測定**するのが望ましい。我々は、作成業者に対して、自分たちの努力だけに集中するのではなく、製品セキュリティに対する努力の結果を客観的に測定して定期的に報告すること、そして、顧客の安全の大幅改善に繋がるソフトウェア開発ライフサイクル(SDLC)の変化を生み出すフィードバックの循環を作ることを呼びかける。報告には、学会やセキュリティ研究コミュニティがハイレベルの傾向を追跡し、エコシステム全体の前進を測ることのできる匿名データを含める必要がある。

この原則の実例

ソフトウェア作成業者とオンラインサービス事業者は、この原則の実施における成功を実証する方法を見つけることが望ましい。第三者が調査できるように、技術データ（artifact）の形で証拠を示せるよう努めることが望ましい。作成業者が強固なセキュアバイデザインプログラムを実施していることを単一の技術データで証明することはできない。作成業者は、さまざまな技術データを示すことで、コミットメントを立証できるのである。このアプローチは、「語るより示せ」の精神にある。

この原則を示すために、ソフトウェア作成業者は、以下のリストのようなステップを検討することが望ましい。署名組織は、セキュアバイデザインの検討を開始した時点では、これらの措置を直ちに実施し、対応する成果物（アーティファクト）を作成できる作成業者はほとんどいないことを認識している。さらに、ソフトウェア作成業者は、顧客がセキュリティ上の利点を最大限享受するため製品を実際にどのように使用するかによって、このリストに優先順位をつける必要がある。

セキュアバイデフォルトのプラクティス

1. **初期パスワードを無くす。**初期パスワードは、毎年多くの攻撃の原因とされている。この恒常的な問題を無くすことにコミットすることは、攻撃者に容易なアクセスをさせないこととなる。作成業者は、同様に、パスワードの長さの最小値や、よく知られた破られやすいパスワードを禁止するなど、どのパスワード慣行を実装すべきか検討する。
2. **実地テストの実施。**技術が進化を続け、複雑化するにつれて、ソフトウェア作成業者が現場でのセキュリティに焦点を当てたユーザーテストを実施し、現場における自社製品のセキュリティ態勢を把握することがますます重要になっている。ユーザー研究がソフトウェア開発の必要条件を定めるのと同様に、ソフトウェア作成業者は、セキュリティの利用者体験（UX）が不十分である箇所を理解するために、セキュリティに焦点を当てたユーザー研究を実施するのが望ましい。ソフトウェア作成業者は、顧客が実際の環境で自社製品をどのように導入し使用しているかを観測することで、セキュリティ機能・制御の使いやすさや有効性についての貴重な知見を得ることができる。こうした知見により、改善すべき領域が特定でき、セキュリティに係る顧客ニーズを満たすように製品を改良することができる。例えば、実地テストの結果は、UX フロー、初期設定、アラート、監視方法を変更するよう示唆するかもしれない。また、実地テストは、セキュリティパッチの適用速度を

遅らせ、設定エラーを減らし、攻撃面を最小化するための製品設計における過去の改善点を示すかもしれない。

- 作成業者は、以下の点を検討することが望ましい。
- 顧客は、セキュリティ強化ガイドを正しく実施しているか。
- 製品の既存のセキュリティ機能は、現場で期待されたとおり機能するか。
- それらの機能は、実際の攻撃を防げるか。
- 被害の可能性をより低減できる機能は何か。

これらの点について深い洞察を得るため、ソフトウェア作成業者は、顧客と協力して、製品がどのように攻撃に耐え得るか確認するためレッドチーム演習の実施を希望するかもしれない。これらの実地テストは、物理的な顧客の敷地内で行うか、仮想的に行うか、プライバシーを保護しつつアプリケーションからのテレメトリを経由して行うか、いずれかである。

3. **セキュリティ強化ガイドのサイズを小さくする。**作成業者は、セキュリティ強化ガイドを簡潔にするか、廃止して、顧客が利用する際に優先すべきセキュリティ対策に集中することによって、顧客のセキュリティ態勢を改善することができる。作成業者は、セキュリティ対策を羅列し顧客を圧倒するのではなく、自社製品が影響を受けやすい上位のセキュリティリスクを特定し、これらのリスクを軽減する方法について明確かつ簡潔なガイダンスを提供するのが望ましい。さらに、作成業者は、顧客の環境に簡単に導入できるスクリプトなど、セキュリティ対策の実施プロセスを簡素化するツールや自動化の手段を顧客に提供するのが望ましい。これらのツールは、元の基準から行われた変更を検証し、明確に示すことができることが望ましい。作成業者は、セキュリティ強化ガイドを簡素なものとし、使いやすいツールと自動化の手段を提供することで、顧客の負担を軽減し、製品が安全な方法で確実に導入される支援をすることができる。そのため、一つの手法として、パレートの法則の実践を検討し、一般的なユースケース（80%）では処理数を減らし、その上で、一般的でないシナリオ（20%）では状況に合ったガイダンスとツールを提供するということもできる。このようにしてソフトウェア作成業者は単純なものは単純なままで、困難なものも対応可能とすることができる。実地テストは、顧客がセキュリティ強化ガイドを発見し、理解し、実施するのにどのくらい時間が掛かるかを測る強力なツールにもなる。作成業者は、管理者が強化ガイドからタスクを実行することに頼るのではなく、どのようにすれば製品がその中で管理者に行動を促せるかを検討することが望ましい。
4. **安全でないレガシー機能の使用を積極的にやめさせる。**明確にアップグレードの方針を後方互換性よりもセキュリティ優先とする。より安全な機能やプロトコルの採用を示すブログを公開し、製品の中で安全でない機能について推奨しない旨明示する。多くの顧客が、最新のネットワーク、アイデンティティ、その他の重要なセキュリティ機能を利用してシステムを最新に保つことが困難であることを実証している。場合によっては、顧客はアップグレードによって既存の機能が機能しなくなることを懸念している。アップグレードを可能な限りシームレスに行うことで、顧客はより頻繁にアップグレードし、セキュリティ修正をより頻繁かつ迅速に入手できるようになる。ソフトウェア作成業者は、顧客を、リスクを軽減するというアップグレードの方向性に積極的に誘導することが望ましい。
5. **注意喚起アラートを導入する。**作成業者は、シートベルト未着用の音を繰り返し出す自動車のシートベルトチャイムと同様、ユーザーや管理者が真に危険な状態にあるときに、適時かつ繰り返し警告を行うことが望ましい。例えば、環境内で非推奨のプロトコルを使用していることを管理者に警告し、アップグレードを提案するというように、である。例えば次のようなことができる。ユーザーや管理者、またはアプリケーション設定が安全でない状態にあるときに、適時に繰り返しアラートを発するよう実装する。安全でないモードであることを管理者に定期的に分かるようにする。追加的な機能として、最高権限を持つ管理者がログインするたびに自分のアカウントに多要素認証（MFA）が設定されていないことを認識するよう求めたり、MFA を有効にするまで特定の主要機能を無効にしたりする。
アラート疲れを作り出さずに、これらの目標を達成できるよう工夫する余地がある。

6. **セキュアな設定テンプレートを作成する。**これらのテンプレートは、組織のリスク選好度に応じて、特定の安全な設定を予めセットすることができる。低／中／高セキュリティのテンプレートを用意するのは単純すぎるかもしれないが、この例では、組織のリスクを管理するために何種類のテンプレートで設定を更新できるかを示している。テンプレートは、作成業者が特定したリスクに関して記載している強化ガイドによってサポートできる。

セキュアな製品開発のプラクティス

1. **安全なソフトウェア開発ライフサイクル（SDLC）枠組みへの適合性を文書にする。**安全な SLDC 枠組みは、人、プロセス、技術にわたる目標と事例を提供する。どの安全な SDLC 枠組みにおける措置を採用したかと使用された代替措置の説明を詳述し公表することを検討することが望ましい。米国内では、NIST のセキュアソフトウェア開発フレームワーク（SSDF）の利用を検討するのが望ましい。SSDF は、チェックリストではなく、「安全なソフトウェア開発のために必要な、基本的、かつ健全な慣行」を記述している。
2. **サイバーパフォーマンス目標（CPG）または同等の適合性を文書にする。**組織が NIST の SSDF 標準に適合していることを証明するとき、その組織は SDLC が十分に理解されたベストプラクティスに基づいていると主張していることと同じである。しかし、強固な SDLC を有するというだけでは十分ではない。また、開発中の製品のセキュリティ特性を操作しようとする悪意のある攻撃者から企業と開発環境を保護する必要がある。これは、理論上の攻撃ではなく、既に実行され、顧客や果ては国家安全保障に悪影響を及ぼしている。組織は、CISA CPG、NIST のサイバーセキュリティ・フレームワーク（CSF）、またはその他のサイバーセキュリティのプログラムの枠組みに対する組織の適合を詳述し公表するのが望ましい。
3. **脆弱性管理。**作成業者の中には、内部または外部で発見された脆弱性にパッチをあてることに重点を置き、それ以上のことはほとんど行っていない脆弱性管理プログラムしか有していないものがいる。より成熟したプログラムは、脆弱性とその根本原因に関する広範なデータ駆動型分析を取り入れ、脆弱性の属性全体を体系的に排除するための措置を講じている。こうした作成業者は、品質計画、品質管理、品質改善、品質測定に関する正式なプログラムを実施し、欠陥管理を単なるセキュリティ問題ではなく、ビジネスの問題として捉えている。これらのプログラムは、他業界における品質や安全に関するプログラムに酷似している。
4. **オープンソースのソフトウェアを責任持って利用する。**オープンソースのソフトウェアを利用する場合には、オープンソースのパッケージを精査し、依存関係に立ち返りコードへの貢献を促進し、重要なコンポーネントの開発とメンテナンスを支援することによって、責任を持つ。参考として、日本の経済産業省（METI）は、「オープンソースソフトウェアの利活用およびそのセキュリティ確保に向けた管理手法に関する事例集」を公開している。
5. **開発者のためのセキュアデフォルトを提供する。**開発者のための安全な基礎的な要素を提供することでソフトウェア開発におけるデフォルトの方法が安全なものになるようにする。例えば、SQL インジェクションの脆弱性が広がり、現実に世界で被害を生んでいるときに、開発者はしっかり維持管理されたライブラリを使用すれば同種の脆弱性を防ぐことが確保される。また、「舗装された道路」や「明るく照らされた道」と表現されるように、この慣行に従っていればスピードとセキュリティが確保され、人的エラーが削減される。
6. **セキュリティを理解するソフトウェア開発者を育成する。**安全なコーディングのベストプラクティスで訓練し、自組織のソフトウェア開発者にセキュリティを理解させる。加えて、採用に関する慣習をアップデートしセキュリティに関する知見を評価したり、大学、コミュニティカレッジ、ブートキャンプ、その他の教育者と協力してセキュリティをコンピュータ・サイエンスやソフトウェア開発のカリキュラムに組み込むことにより、より広範な労働力の変革を促す。

7. **セキュリティインシデントイベント管理（SIEM）とセキュリティ統合調整・自動化・対応（SOAR）との統合をテストする。**実地テストに加えて、理解ある顧客とともに、普及しているSIEMおよびSOARサービス提供事業者と協力し、インシデント対応チームが実際のセキュリティインシデント調査あるいはセキュリティインシデントが疑われる調査においてログをどのように使用するか理解する。ソフトウェア作成業者の多くはインシデント対応の経験がないため、インシデント対応者が期待しているより役に立たないログのエントリを作成する可能性がある。SIEMおよびSOAR技術を実際のインシデント対応専門家と組み合わせて作業することで、ソフトウェア開発チームは、正しく完全に事象を語るログを作成することができるようになる。そうすると、インシデント時の時間短縮や、不確実性を減らすことができる。
8. **ゼロトラストアークテクチャ（ZTA）と整合させる。**製品導入ガイドが例えばNISTのZTAモデルやCISA Zero Trust Maturity Modelと整合していることを確認する。顧客の環境にこれらの原則を取り入れるよう推奨する。

ビジネスプラクティス

1. **追加費用なしでログ記録機能を提供する。**クラウドサービスは、セキュリティ関連のログを追加料金なしで生成し、保存することにコミットすることが望ましい。オンプレミス製品も同様に、セキュリティ関連のログを追加料金なしで生成するのが望ましい。さらに、製品はデフォルトでセキュリティイベントをログに記録することが望ましい。多くの顧客はインシデントが発生するまでそのログの価値を理解できないことが多い。この手法には、サイバーセキュリティの現状認識を行うためにはどのセキュリティイベントをログに記録する必要があるか、顧客はどのようにログ記録を調整できるか、どのくらいの期間ログを保持すべきであるか、どのようにログの完全性とストレージの保護を行うか、どのようにログを分析するか、これらを徹底的にレビューする必要があるかもしれない。場合によっては、このレビューにより、すぐ行動に移すことができるログにするために作成業者にとって妥当な費用で、アプリケーションログの管理構成をリファクタリングする必要性が示されるかもしれない。インシデント対応(IR)の専門家と協力することで、現地調査を行う者にとってログが有用となる可能性を高めることができる。セキュリティ情報イベント管理（SIEM）の項を参照願いたい。
2. **隠れた負担をなくす。**セキュリティやプライバシー機能、または統合に決して追加料金を課さないというコミットメントを公表する。例えば、IDアクセス管理(IAM)と言う概念の中に、Single Sign On(SSO)と呼ばれるサービスがある。作成業者は、彼らの製品をSSOサービス（アイデンティティプロバイダとも呼ばれるが）に接続することで追加費用を請求することがある。この「SSO税」は、多くの中小規模の組織（SMO）にとって、優れた認証アクセス管理を手の届かないものとし、強固なセキュリティ態勢の実現を妨げている。ユーザーがMFAを使用することに追加費用を請求するサービスもある。**セキュリティは贅沢品として価格設定されるのではなく、顧客の権利とみなされることが適当である。**一部の作成業者は、このような機能を求める顧客はほとんどおらず、維持するためにはコストがかかると主張してきた。こうした主張は、クレームや値切りの電話をかけてくる顧客はほとんどいないという事実や、すべての顧客がこれらの機能のメリットを理解しているわけではないこと、さらには、すべての機能には維持費がかかるという事実を無視している。にもかかわらず、可用性やデータの完全性に追加料金を課す作成業者は多くない。これらをサポートする費用は、すべての顧客が支払う価格に予め組み込まれており、シートベルト、衝撃を吸収するステアリングコラム、事故時に人命を救うエアバッグなどが含まれる費用と同様である。
3. **オープンスタンダードを採用する。**特に共通ネットワークおよびIDプロトコルには、オープンスタンダードを実装する。オープンスタンダードが利用できる場合には独自仕様のプロトコルを使用しない。
4. **アップグレードツールを提供する。**多くの顧客は最新バージョンの製品を採用することに躊躇する。これには安全なネットワーク接続など、最新かつより安全な機能導入を含む。ソフトウェア作

成業者は、不確実性やリスクの軽減を支援するツールを提供することにより、新しいアップグレードを受け入れる顧客を増加させることができる。顧客を動機づける方法として、顧客がテスト環境でアップグレードとパッチを試せる無料ライセンスを提供するということもできる。

原則２：徹底的な透明性と説明責任を果たす

説明

ソフトウェア作成業者（作成業者）は、安全でセキュアな製品を提供することに誇りを持ち、その能力によってコミュニティの他の作成業者から差別化を図ることが望ましい。

透明性に関する一般的な懸念をここで説明する。実務者が「徹底的な透明性」について議論すると、「攻撃者のためのロードマップ」を提供しているとの懸念に行き着く傾向がある。しかし、攻撃者はそのようなロードマップなしで攻撃を成功させている多くの証拠があり、そのような懸念は、直接的な顧客、間接的な顧客、サプライチェーン、そしてソフトウェア業界全体に利益をもたらす透明性の二の次とすることが望ましい。

透明性は、業界が同様の慣習、言い換えると「良い慣習」とはどのようなものであるかを確立するのに役立つ。それは、顧客のニーズ、脅威アクターの手法や経済力の変化、技術の進歩に応じて、これらの目安が時とともに変化することを助ける。透明性は、リソースの少ない作成業者が、より成熟した実力のあるリソースを持つ作成業者から学ぶことを支援する。情報共有を語る場合には、リアルタイムの脅威指標だけでなく、次の諸点も含めることが望ましい。

透明性は、セキュリティに関する意思決定を開発プロセスの早い段階で行わせ、経営層、エンジニア、セキュリティ専門家を継続的に活動させることを可能にする。透明性は、製品に説明責任の観点を加えることを可能にする。

「透明性」の前に「徹底的な」という形容詞を選んだことを説明したい。今日、作成業者がソフトウェアをどう開発・保守しているか、また、長年に渡ってデータを使ってプログラムをどう成熟させているか、詳細な情報を公開することは殆ど無い。ソフトウェア業界では、どのようにソフトウェアを設計しているかのガイドツアーを提供する作成業者は殆ど無い。ソフトウェア作成業者は、他社がどのようにSDLCプログラムを作り上げ、顧客環境下でこのプログラムが攻撃者に対して如何に耐えるかを見る機会は殆ど無い。ソフトウェア業界全体として、セキュリティ上の欠陥の費用を測定し、脆弱性の類いを無くす戦略と言った話題の情報共有を積極的に行うことでメリットが得られる筈なのに、である。その結果、すべての作成業者が、製品セキュリティへの対処法を自ら見いださなければならない。それゆえに、セキュリティ機能や安心、安全に追加の負担をかけないことが、利益よりむしろ費用となってしまう可能性がある。企業同士で協力し透明性を確保することにより負担軽減が可能となるかもしれない。

我々は、ソフトウェア業界の深化を加速させる手法に焦点を当てたい。場当たり的で、一歩一歩改善している余裕は最早ないのである。賢く、適応される敵の脅威を皆で克服するためには、現在は心地よくないが、業界全体を前進させるのに必要な水準の透明性を受け入れなければならない。セキュアバイデザイン原則のいくつかを体現している作成業者がある。ウィリアム・ギブスンが言ったように、「未来は既にここにあるが、ただ、あまり均等には配分されていないだけだ」。**徹底的な透明性は、情報の配分を助け、敵よりも守備側に利益をもたらすだろう。**

透明性は、他社がSDLCを成熟させる支援をする以上のことができる。潜在的な顧客や投資家は、作成業者が行った投資やトレードオフについて多くを学ぶことができ、さらに、それらの投資が顧客に作り上げたセキュリティ態勢も学ぶことができる。徹底的な透明性を受け入れる作成業者は、価格や機能だ

けでなくセキュリティについても顧客に情報を提供し、購入の意思決定を助ける。

組織がサプライチェーンとSDLCを保護するために努力しているにもかかわらず、作成業者は、ここ最近、ビルドプロセスでの侵入を許している。徹底的な透明性を受け入れることは、攻撃そのものと、未来の攻撃を検知し防ぐための改善を公に公表することに繋がる。このような情報共有は、他の組織が同様の運命を受けずに学ぶことを助けることとなる。

この原則の実例

この原則を実践するためにソフトウェア作成業者は、以下を含むステップを踏むことが望ましい。

セキュアバイデフォルトのプラクティス

1. **セキュリティ関連の総合的な統計や傾向を公表する。**例として、顧客や管理者の MFA 採用、安全でないレガシーなプロトコルの使用などがある。
2. **パッチ適用の統計を公表する。**製品の最新バージョンを使用している顧客の割合と、更新をより簡単で信頼性の高いものにするための努力を詳しく説明すること。
3. **未使用の管理者特権のデータを公表する。**顧客ベースに対する過剰な権限付与に関する集計情報と、攻撃面を減らすために行っている顧客の行動変容を促す対応やその他の製品の変更を公表する。未使用特権は、シートベルトチャイムのような管理者に対するアラートを行う対象になり得る。

セキュアなプロダクト開発のプラクティス

1. **内部セキュリティ管理の確立。**多くの企業が、データをクラウド事業者に移行することにメリットを感じている。そのクラウド事業者が攻撃者の標的となっている。Software as a Service （SaaS）事業者は、内部管理の統計を公表するのが望ましい。例えば、SaaS 事業者は、Fast ID Online（FIDO）認証のようなフィッシングに耐性のある MFA の内部展開に関する統計を公表するのが望ましい。理想的には、どのスタッフもフィッシング耐性のある MFA で認証しない限り、顧客やその他の機密データにアクセスできないと言えるようにすることである。
2. **高レベルな脅威モデルを公表する。**セキュアバイデザインの製品は、何を誰から守ろうとしているかを記述した脅威モデルの作成から始める。効果的な脅威モデルとは、侵入がどのように広く行われているかに基づき、企業環境と開発環境、さらにはソフトウェア作成業者が意図する顧客環境で使用されることを想定して作成されている必要がある。
3. **安全な SDLC の自己検証の証明を公表する。**NIST SSDF およびその他の類似枠組みに従っている作成業者は、成熟したソフトウェア開発ライフサイクルに向かって積極的に活動していると言える。作成業者が、どの制御措置をどの製品に対して実施したかについての自己検証の証明を公表することは、こうしたベストプラクティスを遵守し、顧客に対してかなりのレベルの自信を持って製品の提供ができるというコミットメントを示すことになる。他の認証スキームには「Israel Cyber Supply Chain Methodology」等がある。
4. **脆弱性の透明性を活用する。**特定の製品の脆弱性を正確かつ完全な CVE エントリーとして公開することを保証するというコミットメントを公表する。脆弱性の根本原因を特定する CWE の分野では、特に、その必要性が高い。公表された CVE データベースがより正確で完全であればあるほど、業界は、どのように製品がより安全になり、どの属性の脆弱性が最も普及しているかを追跡することができる。しかし、CVE をネガティブな指標として捉えようとする誘惑には気をつけなければならない。CVE は、健全なコード解析やテストコミュニティの証でもあるからだ。作成業者がセキュアバイデザインの哲学を導入するにつれ、既存のコードの脆弱性がより広範に見つかり緩和策が取られるため、初期段階においては、生データの CVE 数が増加する可

能性がある。作成業者は、クラス全体の脆弱性に対処するために取った措置やパターンを含む、過去の脆弱性に関する研究を公表するのが望ましい。例えば、ある企業の CVE の大きな割合がクロスサイトスクリプティング（XSS）に関連していた場合、根本原因の分析、対応策（XSS を防ぐウェブテンプレート枠組みへの移行など）、結果を文書化することで、何十年も前から緩和策が理解されている属性の脆弱性の被害に遭わないことを顧客に知らせることができる。

5. **ソフトウェア部品表（SBOM: Software Bills of Material）の公表。**作成業者は自らに関するサプライチェーンを掌握するのが望ましい。組織が各製品の SBOM[2]を作成、維持し、サプライヤにデータを要求し、SBOM を下流の顧客やユーザーに提供することが望ましい。これは、製品の作成に使用する構成要素を理解する誠実な努力や、新たに特定されたリスクに対応する能力を示すことができる。また、サプライチェーン内のモジュールの 1 つに新たな脆弱性が発見された場合、顧客がどのように対応すべきかを理解するのにも役立つ。参考として、日本の経済産業省（METI）は、「ソフトウェア管理に向けた Software Bill of Materials（SBOM）の導入に関する手引」を公開している。透明性は、組み込みデバイスのファームウェアや、AI/機械学習で使用されるデータとモデルにまで及ぶことが望ましい。SBOM は、購入の決定と運用機能を支援するだけでなく、インフラにおいて、悪意のあるサプライチェーン攻撃を検出して対応するため重要な役割を果たす。
6. **脆弱性開示ポリシーの公表。**(1)作成業者が提供する全製品に対するテストや、それらのテストの条件を許可し、(2)当該ポリシーに合致した行動を取っていた際の法的な免責を提供し、(3)決められた期限後に脆弱性の公開を認める、といった脆弱性公開ポリシーを公表する。作成業者は、発見された脆弱性の根本原因分析を実施し、可能な限り、脆弱性の属性全体を排除するための措置を講じることが望ましい。CISA の「Vulnerability Disclosure Policy Template」を参照願いたい。

ビジネスプラクティス

1. **セキュアバイデザインの保証人となる経営層幹部を指名し公表する。**多くの組織では、セキュリティは（品質と同様に）技術チームに委ねられているが、技術チームには、製品のセキュリティを大きく向上させるため構造改革を行う力は限られている。そこでセキュアバイデザインのプログラムを監督するトップ経営幹部を指名し公表することで、製品セキュリティをトップレベルの経営に関わる問題にできる。
2. **セキュアバイデザインのロードマップを公表する。**実地テストの報告の詳細、同じ性質を持つ脆弱性全体を排除するために取られた処置や、他の原則に列挙されている項目を含め、作成業者は、顧客のセキュリティを改善するために SDLC に加えた変更を文書化することが望ましい。品質改善の取組の場合と同様に、セキュリティ改善プログラムには、計画、管理、改善という特有の局面がある。語るよりも示すという精神に基づき、ロードマップと、これらの局面の背後にある詳細を公表することで、製品がセキュアバイデザインであるという信頼を構築できる。作成業者は、有意義な進歩をした後、透明性レポートに詳述できる。こうすることでセキュアバイデザイン原則へのコミットメントを示すだけではなく、実際の証拠を示すことで他者の同様のプログラムを採用するよう鼓舞できる。
3. **メモリ安全性のロードマップを公表する。**作成業者は、既存製品のメモリに安全な言語への移行や新た製品にメモリに安全な言語を使用することで、大きい脆弱性分類の一つを削減するための手順を踏むことができる。これは、すべてのケースにおいて実施することは難しいかもしれないが、一方で、作成業者は、アプリケーション全体を作成し直す代わりに、メモリに安全な言語のラッパーアプリケーション開発することが検討可能である。これは、作成業者が、採用、訓練、コードレビューおよびその他の内部プロセスをどのように更新し、またオープンソースコミュニティが同様のことを行おうとする際に彼らがどのように支援するかが含まれる。

4. **結果を公表する。**セキュアバイデザインの哲学を具現化するためにSDLCを更新する中で、組織は迅速な成功を収める場合や、成功するために多くのリソースを投入する必要がある場合、または、いくつかの予期しない失敗に直面する場合もあろう。内部の成功と失敗を発表することで、その結果から業界全体が学ぶことができる。

原則３：トップ主導

説明

我々は全体的な哲学を「セキュアバイデザイン」と呼んでいるが、顧客の安全に対する動機付けは、設計段階の遥か前から始まっている。それは、経営目標、暗黙および明示的な目的、望ましい成果から始まる。経営幹部がセキュリティを経営上の優先事項としたときのみ、セキュリティを設計要件にする社内インセンティブを与えたり、経営幹部層内の文化醸成をしたりすることが、最良の結果に結びつく。

製品のセキュリティにとって技術的な専門知識は不可欠であるが、それは技術スタッフだけに任せられる問題ではない。それは経営上の優先事項であり、トップから始める必要がある。

作成業者が最初の2つの原則を受け入れ、意味のある技術データを生み出しているのであれば、第3の原則は必要ないのではないかと考える人もいる。企業がどのようにビジョン、使命、価値、文化を確立するかは製品に影響を与えるが、それらはトップと深く関わる問題である。こうした現象は、安全と品質を劇的に向上させた他の産業に見られる。著名な品質専門家であるJ.M.ジュランはこう書いている。

> 品質でリードするためには、経営上層部が個人的に品質管理を担当する必要がある。品質でリードする企業は、いつも経営上層部が自ら指揮を取っていた。例外を知らない[3]。

我々は、セキュリティは製品の品質の一種であると考える。セキュリティと品質維持が、技術スタッフ任せの単なる技術的な機能ではなく、経営上の必須命題となったときに初めて、企業は、顧客のセキュリティニーズにより迅速かつ効率的に対応できるようになる。行動経済学者のセンディル・ムッライナタンは、著書「欠乏（Scarcity）」の中で、最初から仕事が正しく行われるように会社の資源投資がなされなかった失敗の結果について述べており[4]、また、長期のビジネス（および国家安全保障）のコストに関する長年の蓄積は、結局のところ「パッチ」が品質よりもスピードに焦点を当てたというコストの蓄積である。

リーダーシップを持つ経営陣が企業の社会的責任(CSR)プログラムを実施したように、ソフトウェア作成業者の取締役会を含む企業の取締役会が、サイバーセキュリティプログラムを導くより積極的な役割を果たすことが望ましいという認識が高まっている。企業の「サイバー責任（CCR: Corporate Cyber Responsibility）」という用語は、この新たな概念を説明するために使用されることがある。

この原則の実例

この原則の実例は次のとおりであり、ソフトウェア作成業者は、以下のステップを経ることが望ましい。

1. **企業の財務報告にセキュアバイデザインのプログラムの詳細を含める。**作成業者が上場企業の場合は、年次報告にセキュアバイデザインの取組に関する項目を設ける。自動車会社の年次財務報告

には、集権型または分権型の品質・安全委員会に関する情報を含め、ドライバーと同乗者の安全性に関する項目を設けていることが一般的である。財務報告にセキュアバイデザインのプログラムの詳細を記載することで、その組織が顧客のセキュリティと企業の財務成果を結びつけており、単に流行しているからという理由からマーケティング資料で用語を採用しているのではないことを示すことができる。

2. **自組織の取締役会に対し定期的に報告を行う。**企業の取締役会に対する最高情報セキュリティ責任者（CISO）の報告には、通常、現在および計画中のセキュリティのプログラム、脅威、実際にあったセキュリティインシデントの情報やセキュリティインシデントが疑われる情報、企業のセキュリティ態勢および健全性を中心とするその他の最新情報が含まれる。取締役会は、企業のセキュリティ態勢に関する情報を受けることに加え、製品セキュリティおよびそれが顧客のセキュリティに及ぼす影響に関する情報も含めるよう要請するのが望ましい。取締役会は、顧客のリスクを低減するために、CISO だけでなく、他の経営層幹部も頼ることが望ましい。

3. **セキュアバイデザイン担当取締役の権限を強化する。**技術チームが「経営層幹部の了承」を得ている組織と、経営層幹部が標準的なビジネスプロセスを利用して顧客のセキュリティ向上プロセスを自ら指揮している組織とでは、大きな違いがある。「経営層幹部の了承」という用語は、それがトップレベルの経営目標であるということではなく、誰かが顧客のセキュリティプログラムのアイデアを売り込む必要があったことを意味する。この経営層幹部は、顧客のセキュリティ上の成果を達成するための製品投資に影響を与える権限を与えられる必要がある。

4. **企業内部で意味あるインセンティブを作る。**逆のインセンティブを生じさせないように留意しつつ、報酬制度を見直し、顧客のセキュリティ向上を、他の価値ある行動や成果に見合うものとする。セキュアバイデザイン担当取締役から、製品管理、ソフトウェア開発、サポート、営業、法務、その他の各部門に至るまで、顧客のセキュリティ向上に関するインセンティブを、雇用、昇進、給与、賞与、ストックオプション、その他経営プロセスに組み込む。 例えば、ソフトウェア開発者を昇進させる基準を設定する場合は、アップタイム、パフォーマンス、機能の向上などの他の基準とともに、製品のセキュリティ向上を考慮事項に含める。

5. **セキュアバイデザイン委員会を設置する。**業界によっては、品質委員会を設置し、主要部門や事業部門に品質担当者を配置するのが一般的である。集権的にも分権的にもメンバーを集めることで、これらのグループは、組織の深くからきめ細かい情報を得ながら、トップレベルの目標として品質改善に向け取り組むことができる。同様に、セキュアバイデザイン委員会は、組織全体を通して、セキュアバイデザイン目標に対する保証を改善するであろう。

6. **顧客協議会を設立し、発展させる。**多くのソフトウェア作成業者は、さまざまな地域、業種、規模の顧客層で構成される顧客協議会を持っている。このような協議会では、自社製品の導入における顧客の成功や課題について、多くの情報を得ることができる。協議会の議題では、顧客の安全性を取り上げる専用のトピックを設定する。当初は最大の関心事項でなかったとしても構わない。そして、顧客協議会はどこに報告するのか、また導入された製品のセキュリティに関する洞察を得るため参加者をどのように活用するのかを良く考えなければならない。例えば、協議会が、マーケティングや営業、製品管理に偏っていないか。セキュアバイデザイン担当取締役は、このような顧客との対話の方向付けを支援し、実地調査など本ペーパーの他の要素と結びつけることが望ましい。

セキュアバイデザインの手法

Secure Software Development Framework（SSDF）は、米国標準技術研究所（NIST: National Institute of Standards and Technology）の SP 800-218 としても知られ、ソフトウェア開発ライフサ

イクル(SDLC)の各段階に統合できる、高いレベルの安全なソフトウェア開発の慣行が纏められている。これらの慣行を実践することで、ソフトウェア作成業者は、より効果的にリリースされたソフトウェアの脆弱性を発見して除去したり、脆弱性の悪用に関する潜在的な影響を軽減したり、脆弱性の根本原因に対処して将来の再発を防止することができる。

署名組織は、SSDF の実践を参照する原則を含め、セキュアバイデザイン手法を使用するよう推奨している。ソフトウェア作成業者は、自社製品全体で、セキュアバイデザインのソフトウェア開発慣行をより多く取り入れるため書面でのロードマップを作成するのが望ましい。網羅的ではないがロードマップに記載すべきベストプラクティス例の一覧は次のとおり。

- **メモリに安全なプログラミング言語の使用**(SSDF PW.6.1)。メモリに安全な言語の使用を可能な限り優先する。署名組織は、メモリに特化した緩和策はレガシーのコードベースに対する短期的な戦術として有効であると認める。例えば、C/C++言語の改善、ハードウェア緩和策、アドレス空間配置のランダム化(ASLR)、制御フローの整合性(CFI)、ファジングなどが含まれる。しかし、メモリに安全なプログラミング言語の採用は、こうした種類の欠陥を減らすという点でコンセンサスができつつあり、ソフトウェア作成業者は、それらの言語を採用する方法を探ることが望ましい。今日、メモリに安全な言語とは、C#、Rust、Ruby、Java、Go および Swift である。詳細については、NSA のメモリ安全性に関する情報シートを参照願いたい。
- **安全なハードウェア基盤の使用**。きめ細かなメモリ保護を可能にするアーキテクチャ機能の使用をする。例えば、従来のハードウェア命令セットアーキテクチャ(ISAs)に適用可能な Capability Hardware Enhanced RISC Instructions(CHERI)で説明されている機能である。他にもトラステッドプラットフォームモジュールやハードウェアセキュリティモジュールなどもある。詳細については、ケンブリッジ大学の CHERI ウェブページを参照願いたい。
- **セキュアなソフトウェアコンポーネント**(SSDF PW 4.1)。消費者向けソフトウェア製品における安定的なセキュリティを確保するために、十分に安全なソフトウェア部品（例えば、ソフトウェアライブラリ、モジュール、ミドルウェア、フレームワーク）を、検証された商流やオープンソースおよびその他第三者開発者から調達し維持すること。
- **ウェブテンプレート枠組み**(SSDF PW.5.1)。クロスサイトスクリプティングなどのウェブ攻撃を避けるため、ユーザー入力の自動エスケープを実装するウェブテンプレートの枠組みを使用すること。
- **パラメータ化されたクエリ**(SSDF PW 5.1)。クエリにユーザー入力を含めずパラメータ化されたクエリを利用することで SQL インジェクション攻撃を避ける。
- **静的、動的アプリケーションセキュリティのテスト(SAST/DAST)**(SSDF PW.7.2, PW.8.2)。これらのツールを使用し、製品のソースコードおよびアプリケーションの動作を分析し、エラーが発生しやすい動作を検出する。これらのツールは、不適切なメモリ管理からエラーが発生しやすいデータベース・クエリ構成(例えば、SQL インジェクションに繋がるエスケープされていないユーザー入力)といった問題にまで対応する。SAST および DAST ツールは、開発プロセスに組み込むことができ、ソフトウェア開発の一部として自動的に実行することができる。SAST および DAST ツールは、単体テストや統合テストなどの他の種類のテストを補完し、製品が期待されるセキュリティ要件を遵守していることを保証する。ソフトウェア作成業者は、問題が特定された場合、脆弱性に体系的に対処するため根本原因を分析するのが望ましい。
- **コードレビュー**(SSDF PW.7.1, PW.7.2)。製品に組み込まれたコードが、他の開発者によるピアレビューやバグの埋め込みといった品質管理手法を受けて、より高い品質が確保されるよう努める。

- **ソフトウェア部品表（SBOM: Software Bill of Materials)**(SSDF PS.3.2, PW.4.1)。製品に組み込まれるソフトウェア一式を可視化するために SBOM 作成を取り入れる。日本の経済産業省は、「ソフトウェア管理に向けた SBOM の導入に関する手引」と「OSS の利活用とそのセキュリティ確保に向けた管理手法に関する事例集」を公表した。
- **脆弱性開示プログラム**(SSDF RV.1.3)。セキュリティ研究者が脆弱性を報告し、これに対する法的な責任免除（セーフハーバー）を受けることができる脆弱性開示プログラムを確立する。この一環として、サプライヤは、発見された脆弱性の根本原因を決定するためのプロセスを確立するのが望ましい。そのようなプロセスには、この文書にあるセキュアバイデザインの慣行(または類似の慣行)を採用することで脆弱性の混入を妨げたかどうか決定することを含むことが望ましい。
- **CVE の完全性**。ソフトウェアセキュリティ設計上の欠陥を業界全体で分析できるように、公開された CVE には、根本原因や共通脆弱性タイプ一覧（CWE）を含める。すべての CVE が正しく、完全であることを保証するには追加的な時間が掛かるが、すべての作成業者と顧客に利益をもたらすような産業界のトレンドに多様なエンティティが気づくことができる。脆弱性管理の詳細については、CISA の Stakeholder-Specific Vulnerability Categorization(SSVC)ガイダンスを参照願いたい。
- **深層防御**。単一のセキュリティ制御の侵害がシステム全体の侵害につながらないようにインフラを設計する。例えば、利用者権限を厳密に付与し、アクセス制御リストを確実に使用することは、侵害されたアカウントの影響を低減できる。また、ソフトウェアのサンドボックス技術は、脆弱性を隔離し、アプリケーション全体が侵害されないよう制限できる。
- **サイバーパフォーマンス目標（CPG: Cyber Performance Goals)を満たす**。基本的なセキュリティプラクティスを満たす製品を設計する。CISA の Cyber Performance Goals は、組織が実施すべき基本的で最低限のサイバーセキュリティ対策の概要を示している。加えて、組織の態勢を強化するためのその他の手法については、CISA の CPG と類似点を含む英国の Cyber Assessment Framework を参照願いたい。作成業者が CPG を満たさない場合(すべての従業員に対してフィッシング耐性のある多要素認証を要求しないなど)、セキュアバイデザイン製品を提供しているとは見なされない。

署名組織は、これらの変更が組織態勢の大幅な変化であることを認識している。そのため、セキュアバイデザインやセキュアバイデフォルトの導入は、自組織に合わせた脅威モデリング、重要度、複雑さ、およびビジネスへの影響に基づいて優先順位を付ける必要がある。これらは、新しいソフトウェアに導入することができ、追加のユースケースや製品にも対応するよう段階的に拡張することができる。場合によっては、特定の製品における重要性とリスク形態に鑑みると、これらの実践を取り入れるスケジュールを前倒しする価値がある場合がある。そうでなかったとしても、セキュアバイデザインやセキュアバイデフォルトの実践をレガシーなコードベースに導入して、時間とともに修正することができる。

セキュアバイデフォルトの手法

署名組織は、セキュアバイデザイン開発プラクティスの採用に加え、ソフトウェア作成業者に対し、セキュアバイデフォルトの設定を優先した製品とするよう推奨している。これらのソフトウェア作成業者は、製品を刷新するときに、これらの慣行に一致するように製品を更新する努力を行うことが望まし

い。次に例を示す。

- **デフォルトのパスワードを排除する**。製品には、一般的に共有されるデフォルトのパスワードを使用するのは望ましくない。署名組織は、デフォルトのパスワードを排除するために、インストールや設定時に強力なパスワードを使用する、あるいは製品出荷時に唯一無二の強いパスワードを各デバイスに設定するよう管理者に要求する製品を推奨している。
- **管理権限のあるユーザーに対する多要素認証（MFA: Multi Factor Authentication）の義務付け。**多くの企業で、MFA でアカウントを保護していない管理者がソフトウェア利用を管理していることが分かった。管理者が価値の高いターゲットであることを考えると、製品は MFA をオプトインではなくオプトアウトにする必要がある。さらに、管理者がアカウントで MFA を有効にするまで、管理者に MFA への登録を定期的に求めるシステムとする必要がある。オランダの NCSC は、CISA のものと類似したガイダンスを有している。詳細については、MFA の成熟度認証に関するファクトシートを参照願いたい。
- **シングルサインオン(SSO)**。IT アプリケーションは、最新のオープンスタンダードを介してシングルサインオンを実装する必要がある。例えば、セキュリティアサーションマークアップ言語（SAML: Security Assertion Markup Language）や OpenID Connect(OIDC)などがある。この機能は、追加コストなくデフォルトで使用可能にすることが望ましい。
- **安全なログの記録**。高品質の監査ログを追加料金なしで顧客に提供する。監査ログは、潜在的なセキュリティインシデントを検知して対応をエスカレーションするために不可欠である。また、疑いのあるまたは既に確認されたセキュリティインシデントの調査にも不可欠である。セキュリティ情報イベント管理(SIEM)システムに、協定世界時(UTC)や標準タイムゾーンのフォーマット、堅牢な文書化技術を使用するアプリケーションプログラミングインタフェース(API)へのアクセスを提供するなどのベストプラクティスを検討する。
- **ソフトウェア認可プロファイル**。ソフトウェアのサプライヤは、認可されたプロファイルの役割およびその指定された使用例に関する推奨を示すのが望ましい。作成業者は、推奨されたプロファイル認可から逸脱した場合にリスクが増大することを顧客に通知する目に見える警告を含めることが望ましい。例えば、医師はすべての患者記録を閲覧できるが、医療スケジュール管理者は、予約に必要な一定の情報のみにアクセスできるよう制限される、などがある。
- **後方互換性よりも将来を見据えたセキュリティ**。製品セキュリティにリスクをもたらすにもかかわらず、後方互換性のあるレガシー機能が製品に含まれ、有効になっていることがあまりにも多い。後方互換性よりもセキュリティを優先し、仮に互換性を破る変更を引き起こす場合でも、セキュリティチームが安全でない機能を削除する権限を与えることが適当である。
- **セキュリティ強化ガイドを確認し縮小する**。製品に含まれるセキュリティ強化ガイドのサイズを縮小し、ソフトウェアの新しいバージョンがリリースされるにつれて確実にサイズが縮小するようにする。セキュリティ強化ガイドに記載されている内容を製品の初期設定段階で具備されるよう統合する。署名組織は、セキュリティ強化ガイドの縮小は顧客との継続的なパートナーシップの結果であり、これには利用者体験(UX)を含む多くの製品チームによる努力があると認識している。
- **セキュリティ設定の UX に対する影響を考慮する**。新しい設定は、最終的な利用者の認知的負担を増大させるため、それによって得られるビジネス上の利点とともに評価する必要がある。設定は存在しないことが理想的であり、最も安全な設定はデフォルトで製品に予め統合されていることが適当である。設定することが必要な場合、デフォルトの選択は共通の脅威に対して広く安全である必要がある。

署名組織は、これらの変更がソフトウェアの使用方法に運用上の影響を与える可能性があることを認識している。したがって、運用上とセキュリティ上の考慮のバランスをとるために、顧客の意見が不可欠である。我々は、これらのアイデアを組織の最重要製品に優先させるという書面のロードマップと経営層の支援を育むことが、安全なソフトウェア開発慣行に移行する第一歩であると認識している。顧客の意見は重要であるが、署名組織は、顧客が、多くの場合ネットワークプロトコルのような改善された標準を取り入れることに消極的であったり、できなかったりする場合があることを認識している。作成業者が顧客に対し、時代の流れについて行き、永遠に脆弱で居続けないよう誘導することが重要である。

セキュリティ強化ガイドとセキュリティ緩和ガイド

セキュリティ強化ガイドは、製品の開発当初からセキュリティ制御がアーキテクチャに組み込まれていないことに起因するかもしれない。セキュリティ強化ガイドは、こうして攻撃者に安全でない機能を特定し悪用する手がかりを与えかねないのである。多くの組織はセキュリティ強化ガイドの存在を知らないことが多く、機器の設定を安全でない状態のままにしがちである。「セキュリティ緩和ガイド」と言われるこの逆のモデルでは、セキュリティ強化ガイドの代わりに、セキュリティ構成の変更が如何なるセキュリティリスクをもたらすかをリスト化し説明するものである。これらのガイドが正しく使用されるように、明確な言葉でそのトレードオフを説明できるセキュリティ実務者によって書かれることが望ましい。

署名組織は、ソフトウェア作成業者に対し、製品を保護する方法を列挙したセキュリティ強化ガイドを作成するのではなく、セキュリティ緩和ガイドを作成し、セキュアバイデフォルトの取組に移行することを推奨する。ある意思決定に対するビジネスリスクを分かりやすい言葉で説明し、悪意あるサイバー攻撃被害へのリスクに対する組織の意識を高めることができるからである。セキュリティのトレードオフは、セキュリティと他のビジネス上の必要性とのバランスを図りながら、顧客企業の経営層幹部が決めることが適当である。

顧客への提言

署名組織は、顧客組織が、供給するソフトウェア作成業者に対して、その製品がもたらすセキュリティ上の結果について責任を問うことを推奨する。署名組織は、顧客組織の経営層に対し、セキュアバイデザイン、セキュアバイデフォルトの製品を購入することを優先するよう推奨する。具体的には、IT 部門がソフトウェア購入前にそのセキュリティを評価することを義務づけるポリシーを作成し、IT 部門に必要に応じて拒否する権限を明確に与えることである。IT 部門には、セキュアバイデザインとセキュアバイデフォルトの慣行（この文書で概説されているものの他、顧客組織によって作成されたものを含む）に力点を置いた購入基準を作成する権限を与える必要がある。IT 部門はソフトウェアを購入する際にこうした基準を実際に当てはめることとなるが、その際に経営層幹部からの支持が不可欠である。組織として、特定の技術製品に関するリスクを受け入れる決定を行う場合には、正式に文書化し、経営層幹部が承認し、定期的に取締役会に報告されることが望ましい。

企業ネットワーク、認証アクセス管理、セキュリティ運用、対応能力といった組織のセキュリティ態勢を支える重要な IT サービス企業を重要なビジネス機能とみなし、組織の成功にとっての重要性に応じて資金拠出を行うことが適当である。顧客組織は、セキュアバイデザインやセキュアバイデフォルトの慣行を取り入れる作成業者を活用するための能力向上に向けた計画を作成するのが望ましい。

顧客組織は重要な IT サプライヤとの戦略的な関係構築に努力こともできる。こうした関係は、複数のレベルでの信頼を生み、問題解決や優先事項の共有などの手段となる。セキュリティはこうした関係における重要な要素であり、顧客組織は、こうした関係において、公式（例えば、契約やベンダーとの協約）、非公式な面を問わず、セキュアバイデザインとセキュアバイデフォルトの慣行の重要性を強固にするよう努めることが望ましい。顧客組織は、技術サプライヤに対して、内部統制に関する態勢やセキュアバイデザインとセキュアバイデフォルト慣行を取り入れるロードマップに関する透明性を期待するのが望ましい。

IT 部門幹部は、セキュアバイデフォルトを組織の優先事項にするだけでなく、どの製品やサービスがこうした原則を体現しているかを理解できるよう、業界のカウンターパートと協力するのが望ましい。こうした幹部は、作成業者が今後セキュリティの取組を優先するよう、彼らに対する要望を検討することが望ましい。顧客は協力することで作成業者に意味あるインプットを行い、セキュリティを優先させる誘因となるためである。

クラウドシステムを利用する場合には、顧客組織はこうした技術サプライヤとの責任共有モデルというものを確実に理解しなければならない。顧客組織は、顧客としての責任だけということではなく、サプライヤのセキュリティに対する責任も明確にしておく必要がある。顧客組織は、セキュリティ態勢、内部統制、責任共有モデルの下で義務を果たす能力について、透明性の高いクラウド事業者を優先することが望ましい。

免責

この報告の中で情報は情報提供という目的に限り「無保証」で提供される。CISA および署名組織は、あらゆる分析の主題を含め、如何なる商用製品やサービスを承認するものではない。特定の商用団体または商用製品、プロセス、サービス、サービスマーク、商標、作成業者、その他への言及も、CISA や共同署名組織による承認、推奨、贔屓を構成したり暗示したりしない。この文書は CISA による共同イニシアチブであり、そのまま規制の文書としての役割を果たすものではない。

資料

CISA

- CISA’s SBOM Guidance
- CISA’s Cross-Sector Cybersecurity Performance Goals
- Guidelines on Technology Interoperability
- CISA and NIST’s Defending Against Software Supply Chain Attacks
- The Cost of Unsafe Technology and What We Can Do About It | CISA
- Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products (foreignaffairs.com)
- CISA’s Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance
- CISA’s Phishing Resistant MFA Fact Sheets
- Cyber Guidance for Small Businesses | CISA

NSA

- NSA's Cybersecurity Information Sheet on Memory Safety
- NSA's ESF Securing the Software Supply Chain: Best Practices for Suppliers

FBI

- Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective
- The Cyber Threat - Response and Reporting
- FBI's Cyber Strategy

National Institute of Standards and Technology (NIST)

- NIST's Digital Identity Guidelines
- NIST's Cyber Security Framework
- NIST's Secure Software Development Framework (SSDF)

Australian Cyber Security Centre (ACSC)

- ACSC's IoT Code of Practice Guidance for Manufacturers

The United Kingdom's National Cyber Security Centre (UK)

- The UK's Cyber Assessment Framework
- The UK NCSC's Secure Development and Deployment guidance
- The UK NCSC's Vulnerability Management guidance
- The UK NCSC's Vulnerability Disclosure Toolkit
- University of Cambridge's CHERI
- So long and thanks for all the bits - NCSC.GOV.UK

Canadian Centre for Cyber Security (CCCS)

- CCCS's Guidance on Protecting Against Software Supply Chain Attacks
- Cyber supply chain: An approach to assessing risks
- Canadian Centre for Cyber Security's CONTI ransomware guidance

Germany's Federal Office for Information Security (BSI)

- The BSI Grundschutz compendium (module CON.8)
- The international standard IEC 62443, part 4-1
- State of IT-security in Germany report, 2022
- BSI practices of web application security

Netherland's National Cyber Security Centre

- NCSC-NL's Mature Authentication Factsheet

Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC)

- Japan's National Cybersecurity Strategy

Japan's Ministry of Economy, Trade and Industry (METI)

- Guide of Introduction of Software Bill of Materials (SBOM) for Software Management
- Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security

Cyber Security Agency of Singapore

- Technical Advisory on Secure API Development
- CSA SingCERT Vulnerability Disclosure Policy
- CSA SingCERT Incident Response Checklist
- CSA SingCERT Incident Response Playbooks
- CSA Security by Design Framework
- CSA Security by Design Framework Checklist
- CSA Guide to Cyber Threat Modelling
- CSA Cybersecurity Labelling Scheme

Other

- How Complex Systems Fail
- The New Look in complex system failure

参考資料

[1] https://csrc.nist.rip/publications/history/ande72.pdf
[2] https://www.cisa.gov/sbom and SBOMs references in TR 03183-2 https://www.bsi.bund.de/dok/TR-03183
[3] Juran on Quality by Design by J.M. Juran, 1992.
[4] Mullainathan, S., & Shafir, E. (2013). Scarcity: why having too little means so much. First edition. New York, Times Books, Henry Holt and Company.