NIST Special Publication 800-70

後援：米国国土安全保障省

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

# IT 製品のためのセキュリティ設定チェックリストプログラム ーチェックリスト利用者と開発者のための手引き

**Murugiah Souppaya**
**John P. Wack**
**Karen Kent**

コンピュータ　セキュリティ

この文書は下記団体によって翻訳監修されています

IPA 独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

NRI SECURE TECHNOLOGIES

NIST Special Publication 800-70

# IT 製品のためのセキュリティ設定チェックリストプログラム ーチェックリスト利用者と開発者のための手引き

Murugiah Souppaya
John P. Wack
Karen Kent

## コンピュータ　セキュリティ

**米国国立標準技術研究所**
**情報技術ラボラトリ**
**コンピュータセキュリティ部門**
Gaithersburg, MD 20899-8930

2005 **年** 5 **月**


**米国商務省　長官**
*Carlos M. Gutierrez*

**技術管理局　技術担当商務次官**
*Phillip J. Bond*

**米国国立標準技術研究所　所長代行**
*Hratch G. Semerjian*

**この文書は下記団体によって翻訳監修されています**

IPA 独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

NRI SECURE TECHNOLOGIES

*情報セキュリティ技術に関する報告書*

米国国立標準技術研究所（NIST: National Institute of Standards and Technology、以下、NIST と称す。）の情報技術ラボラトリ（ITL: Information Technology Laboratory）は、国家の測定および標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。情報技術ラボラトリは、テストの実施、テスト技法の開発、参照データの作成、実装によるコンセプト実証、技術的分析を通じて、情報技術の開発と生産的利用の発展に努めている。情報技術ラボラトリの責務は、連邦政府の情報システムにおいて、費用対効果の高いセキュリティと国家安全保障関連を除く情報のプライバシーを確保するための技術的、物理的、管理的および運用のための標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、コンピュータセキュリティにおける情報技術ラボラトリの調査、ガイドライン、普及活動と、産業界、政府機関および教育機関との共同活動について報告する。

この文書中で特定される商業的組織、装置、資料は、実験手順または概念を適切に説明するためのものである。したがって、NIST による推薦または保証を意味するものではなく、これらの組織、資料、または装置が、その目的に関して得られる最善のものであると意味しているわけでもない。

**米国国立標準技術研究所、Special Publication 800-70**
**米国国立標準技術研究所、Special Publication 800-70、64 ページ（2005 年 5 月）**
**CODEN: NSPUE2**

この文書は、http://checklists.nist.gov/からダウンロードできる。

コメントは、NIST ITL のコンピュータセキュリティ部門の下記のアドレスに
電子メールまたは通常郵便にて送付願いたい。

checklists@nist.gov

100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

本レポートは、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全に正確であることを保証するものではありません。翻訳監修主体は本レポートに記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。

# 謝辞

本書執筆者である Murugiah Souppaya と John Wack（ともに NIST）、および Karen Kent（Booz Allen Hamilton）は、本書草稿の作成に貢献した Anthony Harris と Paul M. Johnson（ともに Booz Allen Hamilton）に感謝の意を表したい。本書草稿をレビューし、その技術的内容に貢献した同僚たちにも感謝する。本書の執筆全体にわたって鋭く洞察に満ちた助言を与えてくれた Timothy Grance、Jeffrey Horlick、Arnold Johnson、Mark Madsen、Edward Roback、Ron Ross、Michael Rubin、および Carolyn Schmidt（ともに NIST）にも感謝したい。また、Clint Kreitner（インターネットセキュリティセンター）、Chase Carpenter、Kurt Dillard および Jesper Johansson（ともに Microsoft Corporation）、Paul Bartock、Trent Pitsenbarger、および Neal Ziring（ともに国家安全保障局）、Terry Sherald（国防情報システム局）、Glenn Brunette（Sun Microsystems）および、有益なコメントを寄せた Apple Computer, Inc.、エネルギー省、Symantec Corporation の各組織にも感謝の意を表したい。

米国国立標準技術研究所は、NIST の IT 製品のためのセキュリティ設定チェックリストプログラムに対する国土安全保障省の後援と支援に対しても深く感謝する。

# 目次

## 図



## 表

（本ページは意図的に白紙のままとする）

# 要旨

米国国立標準技術研究所（NIST：National Institute of Standards and Technology）は、組織および個人ユーザが IT 製品をより適切に保護できるように、セキュリティ設定チェックリストの開発と普及を推進するため、米国国土安全保障省（Department of Homeland Security、以下、DHS と称す）の後援で、『IT 製品のためのセキュリティ設定チェックリストプログラム：チェックリスト利用者と開発者のための手引き（*Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers*）』を作成した。

セキュリティ設定チェックリスト（ロックダウンガイド、セキュリティ強化ガイド、またはベンチマークと呼ばれることもある）は、特定の運用環境に合わせて製品を設定するための一連の指示を、最も簡単な形式で表現したものである。このリストには、テンプレート、自動化されたスクリプト、そのほかの手順を入れることもできる。通常、チェックリストは IT ベンダーが自社製品について作成するが、コンソーシアム、学術機関、政府機関などの組織がチェックリストを作成することもある。うまくまとめられ、標準化されたチェックリストを使用することによって、IT 製品が脆弱性に起因して危険にさらされる事態を大幅に低減できる。チェックリストは、システムを保護するためのリソースが限られている小規模な組織や個人にとって特に有益である。

この文書は、IT 製品のセキュリティ設定チェックリストの利用者と開発者を対象としている。チェックリストの利用者に対しては、NIST チェックリストプログラムの概要を示し、NIST のリポジトリからチェックリストを取得する方法を説明し、関連する運用環境における脅威の説明とベースラインとなる技術的セキュリティ活動に関する一般的な情報を提供する。チェックリストの開発者に対しては、NIST チェックリストプログラムへの参加に関するポリシー、手順、および一般的な要求事項を説明する。

2002 年施行のサイバーセキュリティ研究開発法（Cyber Security Research and Development Act、公法 107-305）は、NIST に対して「*連邦政府内部で広く使用される（またはその可能性がある）各コンピュータハードウェアまたはソフトウェアシステムに関連するセキュリティリスクを最小限に抑えるための設定とオプション選択を規定したチェックリストを開発し、必要に応じて改訂する*」ことを命じている。また、2003 年に開催された DHS の初めての National Cyber Security Summit（国家サイバーセキュリティサミット）で結成された Technical Standards and Common Criteria Task Force（技術標準および共通基準タスクフォース）の Common Configuration Working Group Report（共通設定ワークグループ報告）[1]は、IT セキュリティ設定チェックリストのために NIST の中央リポジトリを使用することを政府が奨励するように勧告した。この文書は、これを受けて、サイバーセキュリティ法および Federal Information Security Management Act of 2002（2002 年施行の連邦情報セキュリティマネジメント法、以下、FISMA と称す。公法 107-347）に基づくその法的責任を推進するために、NIST により作成された[2]。

## セキュリティ設定チェックリストをなぜ使用するべきなのか？

ユーザのコンピュータには、リモートで起動されたネットワークサービスを悪用する行為から、電子メール、悪意のある Web サイト、ファイルのダウンロードを経由して広がる悪意のコードに至るまで、数多くの脅威が存在する。IT 製品の脆弱性はほぼ毎日のように発見され、すぐに利用できるさまざまな攻撃手法がインターネット上のいたるところで手に入る。多くの場合、IT 製品はさまざまな利用者を想定して作られているため、抑止効果のあるセキュリティ管理策が、通常は、デフォルトで有効になっていない。このため、多くの IT 製品は初期状態のままでは脆弱である。数多くの IT 製品に対して適切なセキュリティ設定を見出すことは、熟練のシステム管理者にとっても、複雑かつ困難で時間のかかる作業である。

IT セキュリティのソリューションは複雑だが、基本的で効果的なツールの 1 つがセキュリティ設定チェ

[1] Technical Standards and Common Criteria Task Force の最終レポートは、http://www.cyberpartnership.org/TF4TechSummary.pdf で入手できる。

[2] サイバーセキュリティ法および FISMA の全文は、http://csrc.nist.gov/policies/HR3394-final.pdf および http://csrc.nist.gov/policies/FISMA-final.pdf でそれぞれ入手できる。

ックリストである。セキュリティ設定チェックリストの開発を容易にし、サイバーセキュリティ法の要求事項を満たすため、NIST は次のようなプログラムを開発した。(a) IT 製品を保護するための標準化された品質の高いチェックリストを開発するための手引きをベンダーやそのほかのグループに提供する。(b) チェックリストを NIST に提出するための公式の枠組みを確立する。(c) チェックリストリポジトリを利用可能にすることで利用者を支援する。

組織や個人は、チェックリストを使用することで次のようなメリットが得られる。

- 一般的で危険なローカルおよびリモートの脅威に対する防御となるセキュリティのベースラインレベル、およびシステムの保護に対する一貫したアプローチ。
- 導入済みの IT 製品の適切なセキュリティ設定に関する研究開発に要する時間の大幅な短縮。
- 小規模な組織が外部のリソースを活用して推奨される実践的なセキュリティ設定を実装できるようにする。
- 一般公開システムに対するセキュリティ侵害による信用喪失や困難を回避する。

セキュリティ設定チェックリストを使用することによって組織の全体的なセキュリティレベルを大幅に改善できるが、システムや製品を 100%安全にするチェックリストは存在しない。しかし、一般的には、ソフトウェアに内在する欠陥やバグからシステムを保護することに重点を置いたチェックリストを使用することにより、製品のセキュリティと将来的な脅威からの保護をより高いレベルで実現できる。

## NIST プログラムの背景にある動機は何か

多くの組織でさまざまなチェックリストが作成されているが、これらのチェックリストは品質や使い勝手の面でばらつきが大きく、ソフトウェアの更新やアップグレードのリリースによってすでに時代遅れになっている可能性がある。また、チェックリストの中央リポジトリが存在しないため、セキュリティチェックリストを見つけるのは困難な作業である。さらに、提供されるセキュリティのレベルがチェックリストによって大きく異なる場合もある。チェックリストが最新かどうかの判断や、チェックリストをどのように実装するべきかの判断が難しい場合もある。既存の多くのチェックリストは品質が高く使い勝手もよいが、多くの利用者は大部分のチェックリストを入手できないか、または有効に使うことができない。

NIST プログラムの目標は、次のとおりである。

- 開発者が NIST にチェックリストを提出するための枠組みを提供することにより、セキュリティ設定チェックリストの開発と共有を促進する。
- 開発者が一般的な運用環境に適合したチェックリストを作成できるように支援する。
- チェックリストの品質と使い勝手を向上させるためのガイドラインを提供することにより、開発者と利用者を支援する。
- チェックリストのレビュー、更新、保守について、管理されたプロセスを提供する。
- 使い勝手のよい、チェックリストのリポジトリを提供する。

NIST のプログラムは、利用者がすぐに利用できるチェックリストを作成するベンダーを支援する役割も果たす。このような場合でも、製品のユーザは導入済みのチェックリストが更新されているかどうかを NIST チェックリストリポジトリで確認することが望ましい。

## 利用者がチェックリストにアクセスするには

NIST は、チェックリストの説明を記載したチェックリストリポジトリを管理している。チェックリストリポジトリは、http://checklists.nist.gov/にある。利用者は、説明を参照し、各種の条件（製品の分類、ベンダー名、提出した組織など）を指定して特定のチェックリストを見つけることができる。この文書では、チェックリスト利用者がチェックリストを取得して IT 製品に適用するときに実行すべき手順を示した。

## 一般的な運用環境とは

NIST は、一般的な運用環境に対応するチェックリストの有用性がきわめて高いことを認識している。NIST チェックリストプログラムは、多くの利用者にとって一般的と思われる広範な運用環境および特殊化された運用環境を特定している。これらの環境を特定して記述することにより、利用者はそれぞれの運用環境に最も適したチェックリストをより適切に選択することができ、開発者はこれらの環境に対応する一般的なセキュリティベースラインに合わせてチェックリストをより適切に設定することができる。次のような運用環境がある。

- **スタンドアロン**環境または**スモールオフィス／ホームオフィス**（**SOHO**）環境は、家庭またはビジネスのために使われる小規模な略式のコンピュータ設置状況を表す。スタンドアロンには、ノート型パソコン、モバイル機器、家庭用コンピュータから、在宅勤務システム、小規模企業、企業の営業所に至るまでの、各種の小規模な環境や機器が含まれる。
- **マネージド**環境または**エンタープライズ**環境は、一般に、一連のハードウェアおよびソフトウェアの設定が規定および体系化され、通常はファイアウォールやそのほかのネットワークセキュリティ機器によってインターネットから保護された集中管理型のワークステーションおよびサーバで構成される大規模組織システムである。
- **カスタム**環境は、セキュリティの機能とレベルが他の環境に当てはまらないシステムを含む。一般に、カスタム環境には次のように「**セキュリティを優先することによる機能制限**」と「**レガシー**」の 2 種類がある。
    - **セキュリティを優先することによる機能制限。**環境内に攻撃やデータ暴露の危険性が高いシステムやネットワークが含まれるため、機能よりもセキュリティが優先される。脅威のレベルが高い環境においては、システムは、（汎用のワークステーションやシステムではなく）その機能が制限または特殊化されていると見なされる。このような環境には、外部に面したファイアウォールや公開の Web サーバのほか、データの内容や任務の目的が重要であるがゆえに、レガシーアプリケーションや他のシステムとの相互運用性などの有用なシステム属性にマイナスの影響が生じる可能性よりもセキュリティのための積極的なトレードオフの方が重視される環境が含まれる。この環境に対するチェックリストは、ホームユーザや大規模な汎用システムには推奨されない。セキュリティを優先することによる機能制限環境がほかの環境のサブセットになっている場合もある。
    - **レガシー。**レガシー環境には、旧式でセキュリティの低い通信メカニズムを使用する可能性がある古いシステムまたはアプリケーションが含まれる。レガシー環境で稼動している他のコンピュータには、レガシーシステムおよびアプリケーションと通信できるように、制限の少ないセキュリティ設定を適用することが必要になる場合がある。レガシー環境がスタンドアロン環境やマネージド環境のサブセットになっている場合もある。

## チェックリスト開発者がプログラムを使用するには

NIST チェックリストプログラムは、チェックリストを一貫した方法で開発するためのプロセスと手引きを

提供する。チェックリスト開発者の手順には、チェックリストの初期開発、チェックリストのテスト、プログラムのガイドラインに沿ったチェックリストの文書化、および NIST へのチェックリストパッケージの提出が含まれる。NIST は、プログラムの要求事項に従ってチェックリストを検査したあと、チェックリストの公開レビューを通常 30～60 日間にわたって行う。チェックリストは、公開レビューの期間とそれに続く問題解決のあと、詳細な説明とともに NIST チェックリストリポジトリ（http://checklists.nist.gov/）に掲載される。NIST は、チェックリストの見直しと必要に応じた更新の提供をチェックリスト開発者に定期的に依頼する。古くなったチェックリストや正確でなくなったチェックリストは、NIST によって廃棄またはアーカイブされる。

## FISMA の要求事項に対応するには

FISMA（第 3544 条（b）（2）（D）（iii））[3]は、各政府機関に対して、受容できる最低限のシステム設定における要求事項を判断し、その要求事項に確実に適合することを求めている。これを受けて、連邦政府機関および連邦政府に製品を納入するベンダーは、NIST のリポジトリを使ってこれらのチェックリストを取得または実装し、共有することが奨励される。

# 1. はじめに

*セキュリティ設定チェックリスト*（ロックダウンガイド、セキュリティ強化ガイド、またはベンチマークと呼ばれることもある）は、定義済みの運用環境に合わせて製品を設定するための一連の指示を、最も簡単な形式で文書化したものである。このリストには、テンプレート、自動化されたスクリプト、そのほかの手順を入れることもできる。チェックリストは、特定の IT 製品や環境を対象とするもので、IT ベンダーだけでなく、コンソーシアム、業界団体、連邦政府機関やそのほかの政府組織、および官民両セクタのそのほかの組織によって開発される。うまくまとめられ、標準化されたチェックリストは、IT 製品の脆弱性に起因して危険にさらされる事態を大幅に低減するのに役立ち、システムを保護するためのリソースが限られている小規模組織や個人にとって特に有益である。

この文書は、IT 製品のセキュリティ設定チェックリストの利用者と開発者を対象としている。チェックリストの利用者に対しては、セキュリティ設定チェックリストとそのメリットを説明し、NIST チェックリストプログラムを使ってチェックリストを検索および取得する方法を説明する。開発者に対しては、NIST チェックリストプログラムへの参加に関するポリシー、手順、および一般的な要求事項を本文および付録で説明する。

安全なネットワークとホストを維持することがかつてないほど重要になっている。あらゆるコンピュータシステムに対する広範囲の電子的な攻撃が当たり前のことになってきた。ユーザのコンピュータには、リモートで起動されたネットワークサービス悪用行為から、電子メール、悪意のある Web サイト、ファイルのダウンロードを経由して広がる悪意のコードに至るまで、数多くの脅威が存在する。IT 製品（オペレーティングシステムやアプリケーションなど）の脆弱性はほぼ毎日のように発見され、すぐに利用できるさまざまな悪用手段がインターネット上のいたるところで手に入る。多くの場合、IT 製品はさまざまな利用者を想定して作られているため、抑止効果のあるセキュリティ管理策が、通常は、デフォルトで有効になっていない。このため、多くの IT 製品は初期設定のままでは脆弱である。

こんにちのシステムや製品はひじょうに複雑で管理がしにくく、セキュリティの確保が困難である。このことが状況をさらに複雑にしている。たとえば、こんにちのパーソナルコンピュータシステムは、一昔前のシステムに比べてはるかに複雑で洗練されており、（大部分とまではいかないが）多くのユーザや管理者に対しては、これらのシステムを支援なしでは安全に管理することは期待できない。数多くの IT 製品の妥当なセキュリティ設定を見出すことは、熟練のシステム管理者にとっても、複雑かつ困難で時間のかかる作業である。しかし、すべてのシステムが脅威に直面しているため、ホームユーザから大企業のエンドユーザに至るすべての利用者にとって、セキュリティはひじょうに重要である。家庭や在宅勤務のユーザのシステムでも、インターネットを使用することで共通の脅威に直面するため、大規模組織で一般的に見られる強力なセキュリティ管理策が有益な場合がある。

IT セキュリティのソリューションは複雑だが、簡単で効果的なツールの 1 つがセキュリティ設定チェックリストである。セキュリティ設定チェックリストの開発を容易にし、2002 年施行のサイバーセキュリティ研究開発法（Cyber Security Research and Development Act、公法 107-305）[1]の要求を満たすため、NIST は次のような目標を持つプログラムを開発した。

- 標準化された品質の高いチェックリストを開発するための手引きによってベンダーやそのほかのグループを支援する。
- チェックリストを NIST に提出するための正式なプログラムを提供する。
- チェックリストリポジトリを用意して利用できるようにすることでチェックリスト利用者を支援する。

この文書では、現在および今後のチェックリスト利用者のために、NIST チェックリストプログラムの概要とチェックリストの取得方法および利用方法を示す。この文書で説明する NIST チェックリストリポジトリは、http://checklists.nist.gov/にある。リポジトリの利用者は、使用中または購入を検討中の IT 製品に関するチェックリストの有無の確認や、同じ IT 製品のために開発されたチェックリスト間の相違の確認、チ

ェックリストの入手先の特定を行うことができる。

チェックリスト開発者のために、この文書では、プログラムを使ってチェックリストを作成し、NIST に提出する方法の概要を示す。また、提出されたチェックリストの NIST による検査の方法、チェックリストの掲載方法と管理方法、問題の解決方法、およびプログラムへの参加と NIST チェックリストロゴの使用に関する管理上の要求事項を示す。

## 1.1 作成機関

サイバーセキュリティ法は、NIST に対して「連邦政府内部で広く使用される（またはその可能性がある）各コンピュータハードウェアまたはソフトウェアシステムに関連するセキュリティリスクを最小限に抑えるための設定とオプション選択を規定したチェックリストを開発し、必要に応じて改訂する」ことを命じている。この文書は、これを受けて、サイバーセキュリティ法および Federal Information Security Management Act of 2002（2002 年施行の連邦情報セキュリティマネジメント法、以下、FISMA と称す。公法 107-347[3]）に基づくその法的責任を推進するために、NIST により作成された。

NIST は、政府機関のすべての業務と資産に十分な情報セキュリティを提供するための標準とガイドライン（最小限の要求事項を含む）を作成する責任を負うが、このような標準およびガイドラインは国家安全保障に関わるシステムには適用されない。このガイドラインは、行政管理予算局（Office of Management and Budget、以下 OMB と称す）の通達（Circular）A-130 の第 8b（3）項『政府機関の情報システムの保護（Securing Agency Information Systems）』の要求事項と一致しており、これは A-130 の付録 IV「重要部門の分析（Analysis of Key Sections）」で分析されているとおりである。補足情報は、A-130 の付録 III[4]に記載されている。

このガイドラインは、連邦政府機関による使用を目的として用意されたが、非政府組織が自己責任において使用することもできる。その場合は出典を明らかにすることが望ましいが、著作権の制約はない（翻訳者注：著作権に関するこの記述は、SP800-70 の英語の原文のことを言っており、日本語へ翻訳した本文書の著作権は、独立行政法人情報処理推進機構および NRI セキュアテクノロジーズ株式会社に帰属する）。この文書におけるいっさいは、商務長官が法的権威に基づき連邦政府機関に対して義務付け、拘束力を有する標準およびガイドラインを否定するものではない。また、これらのガイドラインは、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威を変更したり、これらに取って代わったりするものと解釈されるべきではない。

## 1.2 対象読者と前提条件

この文書は、官民両セクタの現在および今後のチェックリスト利用者および開発者向けに作成されている。チェックリスト開発者には、IT ベンダー、コンソーシアム、業界団体、政府組織、および官民両セクタのそのほかの組織を含む。チェックリスト利用者には、政府機関、企業、小規模企業、そのほかの組織に属するエンドユーザ、システム管理者、IT マネージャのほか、一般市民を含む。

この文書は、読者がコンピュータセキュリティに関わる一般的な考え方と Web を通じて情報を取得する方法に習熟していることを前提としている。

## 1.3 文書の構成

セクション 2 では、チェックリストの概要を示し、NIST チェックリストプログラムの利点と仕組みを説明する。また、この文書のほかのセクションに詳細な説明がある場合は、その参照先を示す。

セクション 3 では、定義済みのチェックリスト運用環境、脅威の説明、およびベースラインとなる技術的セキュリティ活動の詳細を示す。これらは、NIST チェックリストプログラムで使用され、開発者がこれらのセキュリティ活動に合致するチェックリストを作成するのに役立っている。チェックリスト利用者も、セクション 3 の資料を適用することにより、ベースラインとなるセキュリティ活動を十分に理解し、それぞれの運

用環境に最も合うチェックリストを選択することができる。

セクション 4 では、今後のチェックリスト利用者のための情報を示す。特定されたニーズに最も合うチェックリストを NIST チェックリストプログラムで検索および取得する方法を説明する。また、チェックリストの実装（特定の運用環境の分析と必要に応じたチェックリストの調整を含む）に関する手引きも示す。

セクション 5 では、現在および今後のチェックリスト開発者に対する手引きを示す。この手引きには、チェックリストを準備し、チェックリストリポジトリへの組み入れを求めて NIST にチェックリストを提出するための手順に関する情報が含まれる。

付録 A では、この文書で使用した参考文献を示す。

付録 B では、NIST リポジトリ内のチェックリストの目録を作成するために使われたチェックリスト明細フィールド群について説明する。

付録 C では、NIST チェックリストプログラムへの参加時に満たす必要があるプログラム要求事項と法的要求事項を示す。

付録 D では、NIST チェックリストプログラムの参加およびロゴ使用の契約書式を示す。

付録 E では、この文書で使用している用語の解説を示す。

（本ページは意図的に白紙のままとする）

# 2. NIST セキュリティ設定チェックリストプログラム

このセクションでは、NIST チェックリストプログラムの概要を示す。最初に、チェックリストの内容を説明し、チェックリストが作成される頻度の高い IT 製品の種類の例を示す。次に、セキュリティ設定チェックリストによって得られるメリット（組織のセキュリティのベースラインレベルが向上するなど）を説明する。また、NIST チェックリストプログラムの目標とメリット（チェックリストの品質、使い勝手、可用性の向上など）も説明する。このセクションでは、チェックリストの利用者と開発者の手順の概要、運用環境の種類の概要、および設定チェックリストの使用に関係する FISMA 関連の手引きの要約も示す。手順と環境定義の詳細については、以降の各セクションで説明する。

## 2.1 セキュリティ設定チェックリストとは

*セキュリティ設定チェックリスト*（ロックダウンガイド、セキュリティ強化ガイド、セキュリティガイド、セキュリティ技術実装ガイド（STIG）、またはベンチマークと呼ばれることもある）[3]は、基本的に、運用環境に合わせて IT 製品を設定するための指示や手順を記載した文書である。チェックリストは、IT ベンダーだけでなく、コンソーシアム、学術機関、業界団体、連邦政府機関やそのほかの政府組織、および官民両セクタのそのほかの組織によって開発される。チェックリストには次の任意の要素が含まれる。

- 各種のセキュリティ設定を自動的に設定する設定ファイル（実行可能ファイル、設定を変更するセキュリティテンプレート、スクリプトなど）
- チェックリスト利用者に IT 製品を手動で設定する方法を示す文書（テキストファイルなど）
- 機器を安全にインストールおよび設定するための推奨される方法を説明する文書
- 監査、認証メカニズム（パスワードなど）、境界セキュリティなどの事項に関するガイドラインを記載したポリシー文書

セキュリティ設定チェックリストのすべての指示がセキュリティ設定のために必要であるとは限らない。IT 製品のセキュリティの改善に密接な関係がある管理活動がある場合は、それをチェックリストに含めることもできる。多くの場合、システムに対する攻撃が成功するのは、不十分な管理活動（デフォルトのパスワードを変更していない、古いパッチを適用していないなど）の必然的な結果である。

通常、システム管理者やエンドユーザは、チェックリストの指示に従い、チェックリストに提示されているセキュリティのベースラインレベルに合わせて製品やシステムを設定する。システム管理者は、ローカルセキュリティポリシーを組み込むためにチェックリストを変更する必要に迫られる場合がある。

セキュリティチェックリストの対象となる機器およびソフトウェアの種類の例を次に示す。

- 汎用のオペレーティングシステム
- 一般的なデスクトップアプリケーション（電子メールクライアント、Web ブラウザ、ワードプロセッサ、パーソナルファイアウォール、ウイルス対策ソフトウェアなど）
- インフラストラクチャ機器（ルータ、ファイアウォール、仮想プライベートネットワーク（VPN）ゲートウェイ、侵入検知システム（IDS）、ワイヤレスアクセスポイント（WAP）、遠隔通信システムなど）
- アプリケーションサーバ（ドメインネームシステム（DNS）サーバ、動的ホスト設定プロトコル（DHCP）サーバ、Web サーバ、簡易メール転送プロトコル（SMTP）サーバ、ファイル転送プロトコル（FTP）サーバ、データベースサーバなど）

[3] これ以降、設定チェックリスト（他の文献でロックダウンガイド、セキュリティ強化ガイド、またはベンチマーク設定と呼ばれるもの）を表す場合は、サイバーセキュリティ法の用語である「*チェックリスト*」を使用する。

- そのほかのネットワーク機器（モバイル機器、スキャナ、プリンタ、コピー機、ファックス複合機など）

## 2.2 セキュリティチェックリストを使用するメリットとは

正しく開発されたセキュリティ設定チェックリストは、利用者が、導入済みの初期デフォルト値よりも強固な保護機能を提供するセキュリティベースラインに合わせて IT 製品を設定する際に、大いに役立つ。チェックリストの使用に関連するメリットの例を次に示す。

- 一般的で危険なローカルおよびリモートの脅威（ウイルスやワーム、サービス不能攻撃（DoS）、無許可のアクセス、不正使用など）に対する防御となるセキュリティのベースラインレベルが提供される。
- 組織内の専門知識が盛り込まれた既存のチェックリストを活用することにより、導入済みの IT 製品の適切なセキュリティ設定の研究開発に要する時間が大幅に短縮される。
- 小規模な組織が外部のリソースを活用して推奨される実践的なセキュリティ設定を実装できるようになる。
- 一般公開システムに対するセキュリティ侵害による信用喪失や困難が回避される。

セキュリティ設定チェックリストを使用することによって組織の全体的なセキュリティレベルを大幅に改善できるが、システムや製品を 100%安全にするチェックリストは存在しない。しかし、一般的には、ソフトウェアに内在する隠れた欠陥やバグからシステムを保護することに重点を置いたチェックリストを使用することにより、製品のセキュリティと将来的な脅威（ゼロデイ脆弱性など）からの保護をより高いレベルで実現できる。IT ベンダーが FISMA 関連のセキュリティ管理策のベースラインを順守するための「すぐに使える」推奨チェックリストを提供することにより、連邦政府機関内の構成設定に高い一貫性が確保されるだけでなく、政府機関がチェックリスト開発者によって提供された元のチェックリストを変更することによって特定のアプリケーションや運用環境に合わせて構成設定を微調整しなければならない場合でも、費用対効果のきわめて高い方法で最低限の構成設定を確立することができる。

## 2.3 NIST チェックリストプログラム

多くの組織でさまざまなチェックリストが作成されているが、これらのチェックリストは品質や使い勝手の面でばらつきが大きく、ソフトウェアの更新やアップグレードのリリースによってすでに時代遅れになっている可能性がある。また、チェックリストの中央リポジトリが存在しないため、セキュリティチェックリストを見つけるのは困難な作業である。さらに、提供されるセキュリティのレベルがチェックリストによって大きく異なる場合もある。チェックリストが最新かどうかの判断や、チェックリストをどのように実装するべきかの判断が難しい場合もある。既存の多くのチェックリストは品質が高く使い勝手もよいが、多くの利用者は大部分のチェックリストを入手できないか、または有効に使うことができない。

NIST のプログラムは、チェックリストを体系的で使い勝手のよいものにする役割を果たす。NIST プログラムの目標は、次のとおりである。

- 開発者が NIST にチェックリストを提出するための枠組みを提供することにより、チェックリストの開発と共有を促進する。
- 同じ環境（つまり、セキュリティレベルを同じにする必要がある Microsoft Windows®ベース、UNIX ベース、および Linux ベースのシステムで構成されるネットワーク）に接続されたさまざまな種類のシステムを保護するための一貫したアプローチを提供することにより、開発者を支援する。
- チェックリストの品質と使い勝手を向上させるためのガイドラインを提供することにより、開発者と利用者を支援する。

- チェックリストのレビュー、更新、保守について、管理されたプロセスを提供する。
- 使い勝手のよい国家的なチェックリストのリポジトリを提供する。

### 2.3.1 NIST チェックリストプログラムに掲載されるチェックリストの種類

NIST チェックリストプログラムは、***特定の***IT 製品に対応するチェックリスト（特定のブランドおよびモデルのルータのチェックリストなど）を扱っている。チェックリストには、他のチェックリストを参照するものもある。たとえば、データベース製品のチェックリストから、そのデータベース製品が動作するオペレーティングシステムのチェックリストを参照している場合がある。

NIST チェックリストプログラムは、軍関連を除く政府機関が FISMA の要求事項に対応するのに役立つ。これについては、2.4 項で詳しく説明する。また、このプログラムには、幅広い種類の特殊なニーズに対応するチェックリスト[4]（たとえば、1996 年の医療保険の相互運用性と説明責任に関する法律（HIPAA：Health Insurance Portability and Accountability Act）[5]や 2002 年の米国企業改革法（Sarbanes-Oxley Act）[6]などの規程の要求事項の順守に関連するチェックリストなど）を掲載することもできる。

NIST チェックリストリポジトリは http://checklists.nist.gov/）にある。このリポジトリには、プログラムの要求事項に合わせて開発および検査されたチェックリストが含まれている。利用者は、チェックリストの説明を参照し、各種のフィールド（製品の分類、ベンダー名、提出した組織など）を指定して特定のチェックリストを検索し、入手することができる。

### 2.3.2 利用者および開発者の手順

チェックリストの利用者および開発者に関わる一般的な手順を図 2-1 および図 2-2 に示す。チェックリスト利用者の手順は、次のようにごく簡単である。

- 手順 1 では、利用者がローカルな要求事項（IT 製品、運用環境、関連するセキュリティニーズなど）を収集し、ニーズに最も適した IT 製品を調達または購入する。
- 手順 2 では、利用者がチェックリストリポジトリを参照し、ユーザの運用環境とセキュリティ要求事項に一致するチェックリストを取得する。初期状態のままでセキュリティが確保される製品（ベンダーがセキュリティ設定チェックリストを使ってセキュリティを確保した製品）についても、チェックリストの更新がないかどうかをリポジトリでチェックすることが重要である。
- 手順 3 では、ローカルポリシーと機能的な要求事項を考慮に入れるために必要に応じてチェックリストの調整と文書化を行い、チェックリストをテストし、NIST およびチェックリスト開発者に対してフィードバックを提供する。
- 最後の手順 4 では、チェックリストを導入するための準備（設定やデータのバックアップなど）を行い、実運用環境にチェックリストを適用する。

セクション 4 では、各手順に関して考慮すべき事項を詳しく示す。付録 B には、チェックリストを参照するときに使用するチェックリスト明細フィールドの要約を示す。

[4] このプログラムには、一般的な技術分野（ファイアウォールやルータなど）のベストプラクティスを記述したチェックリストは**掲載されない**。NIST は、ベストプラクティスのチェックリストのディレクトリや他のチェックリストの場所へのリンクを http://csrc.nist.gov/pcig/ppsp.html で管理している。

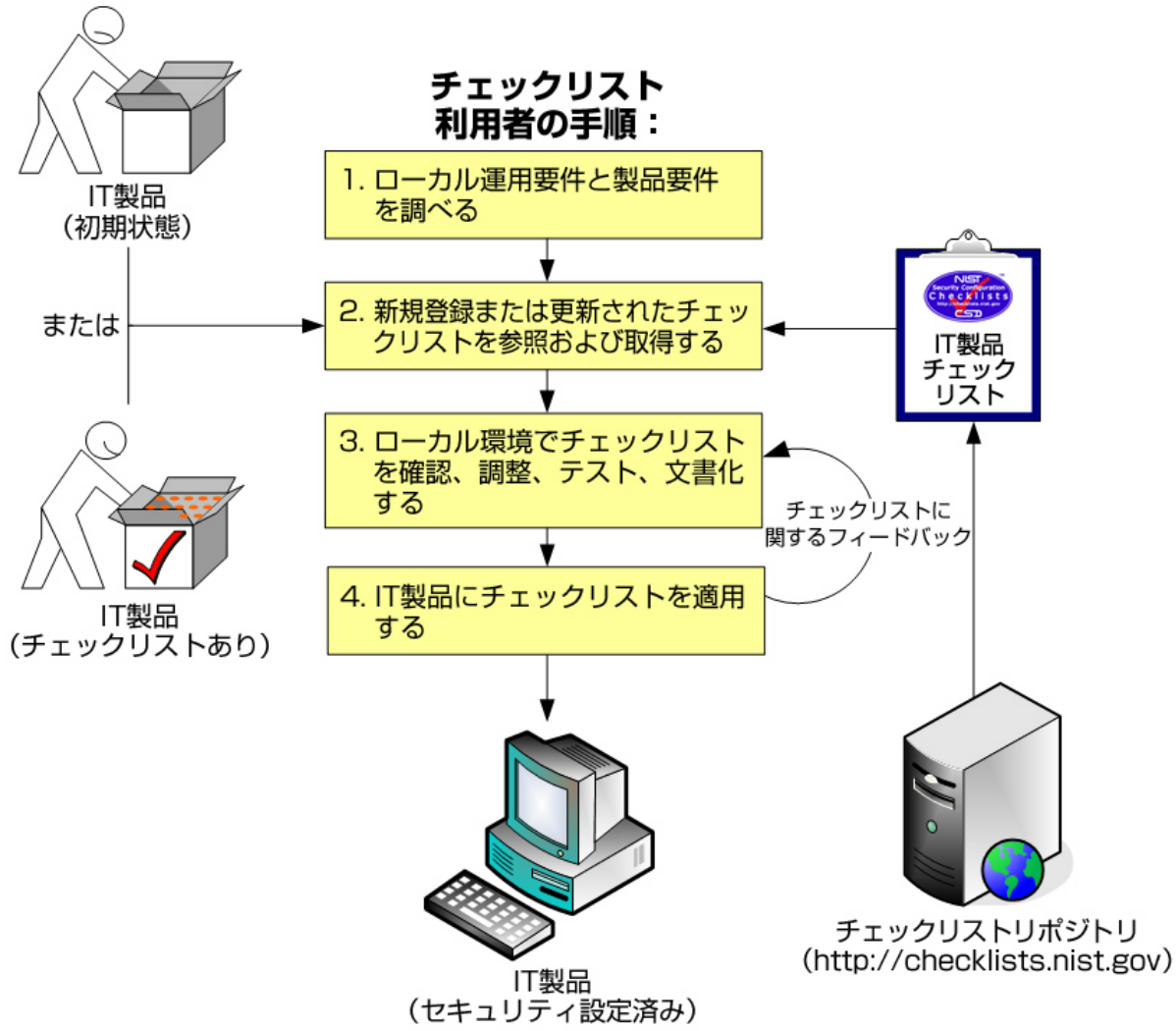


**図 2-1：チェックリスト利用者の手順**

開発者のプロセスは 2 つの段階からなる。第 1 段階では開発者の作業だけが行われ、第 2 段階では NIST、開発者、および一般レビュー者のあいだでやりとりが行われる。第 1 段階には、図 2-2 に示すように 4 つの手順が含まれる。

- 手順 1 では、開発者がチェックリストプログラムの手順と要求事項を確認し、プログラムに参加するための協定に同意する。
- 手順 2 では、開発者がチェックリストを作成、テスト、調整する。
- 手順 3 では、開発者がプログラムのガイドラインに従ってチェックリストを文書化する。
- 手順 4 では、開発者がチェックリスト提出パッケージを準備し、それを NIST に提出する。

第 2 段階では、NIST が開発者や一般レビュー者とやりとりしながら、次のように残りの 4 つの手順を実施する。

- 手順 5 では、NIST がプログラムの要求事項に従ってチェックリストを検査し、問題があれば開発者とともに解決する。

- 次の手順はチェックリストの公開レビューであり、通常 30～60 日間にわたって行われる。レビュー期間中に提出されたコメントには、開発者または NIST が必要に応じて対応する。
- 手順 7 では、NIST がチェックリストをリポジトリに掲載し、そのことを告知する。
- 最後の手順 8 では、チェックリストの定期的な更新とチェックリストのアーカイブへの発行が行われる。

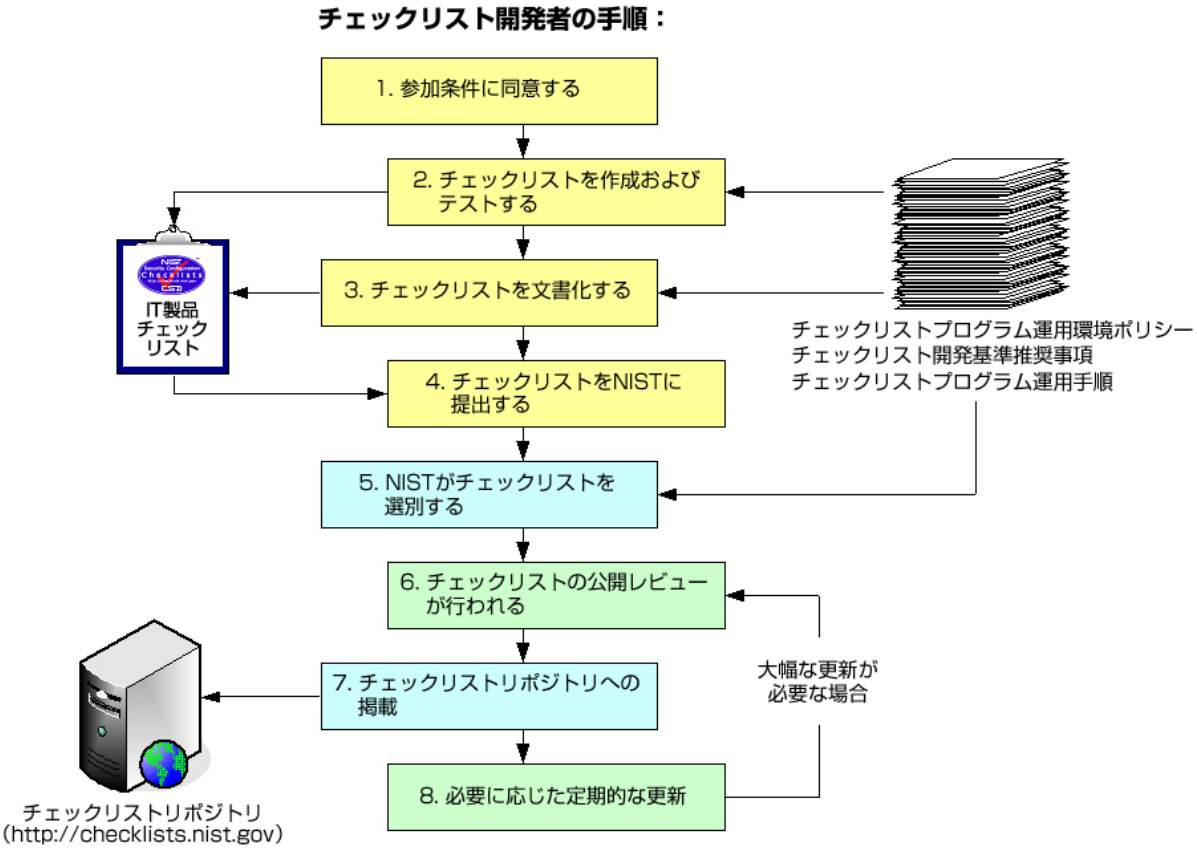


**図 2-2：チェックリスト開発者の手順**

チェックリストの開発手順、および NIST によるチェックリストの検査と公開のプロセスについては、セクション 5 および付録 C で詳しく説明する。

### 2.3.3 一般的な運用環境

チェックリストは、一般的な運用環境に関連付けることができればきわめて有効である。しかし、これらの環境を詳細に指定することは困難か、またはおそらく不可能である。幅広い利用者にとって有効なものするためには、必然的に一般的なものにせざるを得ない。NIST チェックリストプログラムは、多くの利用者にとって一般的と思われる広範な運用環境および特殊化された運用環境を特定している。これらの環境を特定して記述することにより、開発者はこれらの環境に対応する一般的なセキュリティ要求事項に合わせてチェックリストをより適切に設定することができる。また、エンドユーザはそれぞれの運用環境に最も適したチェックリストをより適切に選択することができる。

次のような運用環境がある。

- **スタンドアロン**環境または**スモールオフィス／ホームオフィス** (SOHO) 環境は、家庭またはビジネスのために使われる小規模な略式のコンピュータ設置状況を表す。スタンドアロンに

は、ノート型パソコン、モバイル機器、家庭用コンピュータから、在宅勤務システム、小規模企業、企業の営業所に至るまでの、各種の小規模な環境や機器が含まれる。

- **マネージド**環境または**エンタープライズ**環境は、一般に、一連のハードウェアおよびソフトウェアの設定が規定および体系化され、通常はファイアウォールやそのほかのネットワークセキュリティ機器によってインターネットから保護された集中管理型のワークステーションおよびサーバで構成される大規模組織システムである。
- **カスタム**環境は、セキュリティの機能とレベルが他の環境に当てはまらないシステムを含む。一般に、カスタム環境には次のように「**セキュリティを優先することによる機能制限**」と「**レガシー**」の 2 種類がある。
    - **セキュリティを優先することによる機能制限。**環境内に攻撃やデータ暴露の危険性が高いシステムやネットワークが含まれるため、機能よりもセキュリティが優先される。脅威のレベルが高い環境においては、システムは（汎用のワークステーションやシステムではなく）その機能が制限または特殊化されていると見なされる。このような環境には、外部に面したファイアウォールや公開の Web サーバのほか、データの内容や任務の目的が重要であるがゆえに、レガシーアプリケーションや他のシステムとの相互運用性などの有用なシステム属性にマイナスの影響が生じる可能性よりもセキュリティのための積極的なトレードオフの方が重視される環境が含まれる。この環境に対するチェックリストは、ホームユーザや大規模な汎用システムには推奨されない。セキュリティを優先することによる機能制限環境がほかの環境のサブセットになっている場合もある。
    - **レガシー。**レガシー環境には、旧式でセキュリティの低い通信メカニズムを使用する可能性がある古いシステムまたはアプリケーションが含まれる。レガシー環境で稼動している他のコンピュータには、レガシーシステムおよびアプリケーションと通信できるように、制限の少ないセキュリティ設定を適用することが必要になる場合がある。レガシー環境がスタンドアロン環境やマネージド環境のサブセットになっている場合もある。

図 2-3 に、代表的なスタンドアロン環境、マネージド環境、およびカスタム（セキュリティを優先することによる機能制限）環境を示す。各環境とその一般的なセキュリティベースラインの詳細は、セクション 3 に示す。

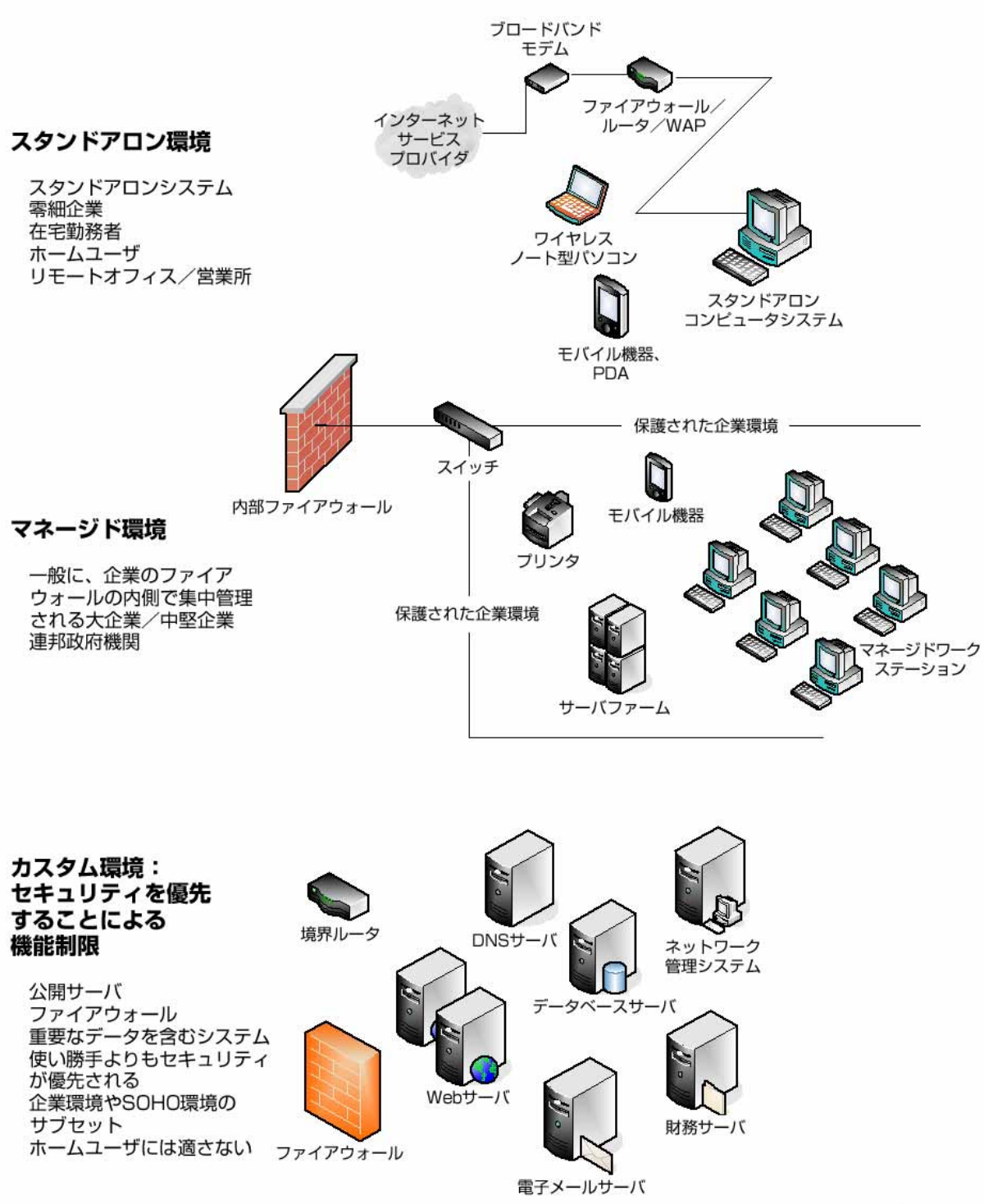


**図 2-3：NIST チェックリストプログラムの運用環境の例**

## 2.4 連邦政府機関が FISMA の要求事項に対応するためのチェックリスト

セキュリティ設定チェックリストは、連邦政府機関が FISMA のセキュリティ要求事項に対応するのに役立つ。FISMA（第 3544 条（b）（2）（D）（iii））[3]は、各政府機関に対して、受容できる最低限のシステム設定における要求事項を判断し、その要求事項に確実に適合することを求めている。これを受けて、連邦政府機関および連邦政府に製品を納入するベンダーは、NIST のリポジトリを使ってこのようなチェックリストを取得または開発し、共有することが奨励される。これらのチェックリストを開発して共有することにより、連邦政府内で広く使用されている IT 製品（一般的なオペレーティングシステムやサーバ、クライアントアプリケーションなど）に対して、いわば「車輪を再発明する」ような無駄な労力を大幅に減らせる。

# 3. NIST チェックリストプログラムの運用環境

NIST チェックリストプログラムは、多くの利用者にとって一般的と思われる包括的な運用環境とカスタマイズされた運用環境を特定している。これらの運用環境には、それぞれ一般的な脅威の説明とベースラインとなる技術的セキュリティ活動がある。

IT 製品のユーザは、ユーザ自身のセキュリティ要求事項やニーズ（その要点については、セクション 4 で詳しく説明する）を最初に特定するときに、このセクションを参照すると役に立つ場合がある。開発者は、チェックリストを作成するときにこのセクションが役に立つ場合がある。これらの環境および環境のポリシーに合わせてチェックリストの開発を調整することにより、これらの環境に対応する一般的で均質な技術的セキュリティ活動と設定に従いながら、さまざまな製品のチェックリストを作成することができる。これについては、セクション 5 で詳しく説明する。

包括的な環境は 2 つあり、それぞれ**スタンドアロン**（またはスモールオフィス／ホームオフィス（SOHO））および**マネージド**（またはエンタープライズ）と呼ばれる。**カスタム**環境は、包括的な環境のサブセットになっている場合もあるが、一般に**セキュリティを優先することによる機能制限**と**レガシーの** 2 つがある。以降の各項では、これらの環境を説明するとともに、脅威とベースラインとなる技術的セキュリティの推奨事項を説明する。

運用環境に関する基準は定期的に更新されるため、開発者はチェックリストを NIST に提出する前にこの文書の最新版を持っているかどうかを確認するべきである。最新版は、http://checklists.nist.gov/から独立したファイルとして入手できる[5]。

## 3.1 背景

あるものを保護する場合、軽減する必要がある脅威を最初に規定することが最も重要である。潜在的脅威を知ることは、この文書のために選ばれた各種のベースライン技術的セキュリティ活動の背後にある根拠を理解する上で重要である。

環境ごとの脅威の考察は、それぞれの環境およびそれらに対応するベースラインの活動を選択するときに考慮された主要な脅威の分類を表している。データやリソースに対する脅威の多くは、過失によって発生する可能性がある。過失には、オペレーティングシステムやアプリケーションソフトウェアの内部で悪用可能な脆弱性を生み出すバグと、エンドユーザや管理者が引き起こすエラーがある。脅威には、意図的な主体（システム上の情報にアクセスしたがっている攻撃者など）または意図的でない主体（雇用が終了した従業員のユーザアカウントを無効にするのを忘れた管理者など）が関わっている。脅威には、ローカル（不満を持つ従業員など）のものと、リモート（別の地域にいる攻撃者）のものがある。チェックリストを使用する組織は、NIST の『IT システムのためのリスクマネジメントガイド（Risk Assessment Guide for Information Technology Systems）』[12]で説明されているように、リスクアセスメントを実施することにより、システムに対する具体的な脅威を明らかにし、脅威に対抗する既存のセキュリティ管理策の効果を判定する。次に、リスク軽減策を実施して、どのような追加手段を（もしあれば）導入するべきかを決定する。この手順を実行することにより、各組織は自組織のニーズを十分に把握し、選択したチェックリストの変更や拡張が必要かどうかを適切に判断できる。

チェックリストの環境のベースラインとなる技術的セキュリティ活動は、各種の NIST Special Publication [8]、[10]、[23]、およびそのほかのソース（国防総省の『Information Assurance Technical Framework（情報保証の技術的枠組み）』[32]など）に掲載されている、一般的に認められた技術的なセキュリティの原則と活動に基づいている。特に、NIST Special Publication 800-27『Engineering Principles for Information Technology Security (A Baseline for Achieving Security)』[11]には、IT セキュリティ機能

[5] NIST は、新しい情報の入手に伴って、この文書に含まれる運用環境に関する基準や情報およびそのほかの基準を更新することがある。

の設計、開発、実装に対するより一貫した構造化されたアプローチを構成するための基礎となるシステムセキュリティに関する一連のエンジニアリングの原則が記載されている。詳細については、開発者がチェックリストを作成するときに推奨されるセキュリティ関連の基準を詳しく説明した 5.1 項を参照されたい。

## 3.2 スタンドアロン環境

**スタンドアロン**環境は、**スモールオフィス／ホームオフィス** (SOHO) とも呼ばれ、小規模な略式のコンピュータ設置状態を表す。この環境には、時折作業に使われる家庭用コンピュータから、企業などで技術上または業務上の理由からリモート管理されていない別の地域にある営業所まで、さまざまな種類の運用設定が含まれる。図 3-1 に、典型的なスタンドアロンネットワークアーキテクチャを示す。

スタンドアロン環境では、次のようなエンドユーザと運用設定が想定される。

- スタンドアロンシステムを所有し、一般にダイヤルアップまたは高速回線経由でインターネットにアクセスするホームユーザで、有線接続またはワイヤレスのホームネットワークを使用する場合もあれば、ネットワーク経由でリソースを共有する場合もある。
- スタンドアロンシステムを使ってホームオフィスで作業する在宅勤務者。
- 一般にファイアウォールによって直接的なインターネットアクセスから保護されたスタンドアロンのデスクトップシステムと小規模オフィスサーバを所有するが、場合によってはデスクトップシステムおよび製品の小規模な集中管理型ネットワークを含み、一般には公的にアクセス可能なサーバを維持管理しない小規模企業。
- 同様の機能を持つそのほかの小規模組織。

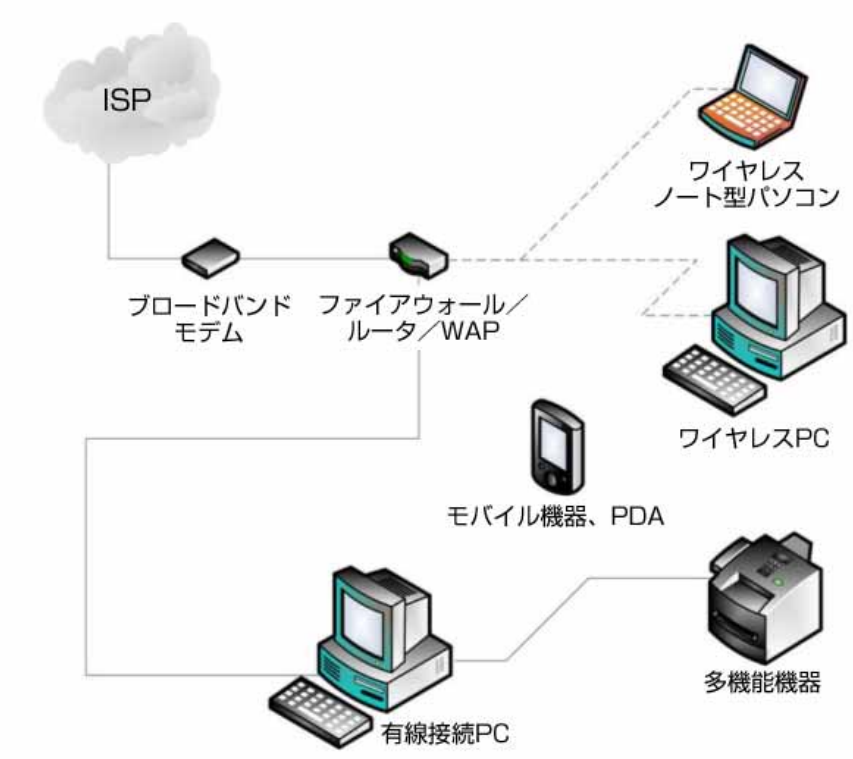


**図 3-1：ホームオフィスのスタンドアロン環境の例**

スタンドアロン環境は、一般にセキュリティのレベルが最も低い。スタンドアロンシステムの管理を行う人は、セキュリティに関する知識が乏しいことが想定される。この結果、機能に重点が置かれ、必要なレ

ベルのセキュリティが確保されていない環境が多い。ネットワークベースのセキュリティ管理策（ファイアウォールなど）が存在せず、スタンドアロンシステムが外部の脅威に直接さらされている場合もある。スタンドアロン環境は悪用の標的にされることが多く、その目的は、情報の入手だけではなく、他のコンピュータを攻撃することである場合もある。また、ワームの増殖による副次的損害である場合もある。

スタンドアロン用のチェックリストは、ホームユーザや小規模組織の任命されたばかりのシステム管理者が理解して実施できるように、比較的単純なものであるべきである。

### 3.2.1 脅威の考察と推奨される技術的セキュリティ活動

スタンドアロン環境における主な脅威は外部に由来し、スタンドアロンの機器は一般にマネージドシステムやセキュリティを優先することによる機能制限システムより制限の少ないセキュリティポリシーを持っているため、スタンドアロンシステムはリモートの脅威として分類される攻撃に対して最も脆弱な傾向がある。スタンドアロンシステムにローカルアクセスできる人数は一般に少ないため、ローカルの脅威は比較的重大でないことが多いが、ローカルやそのほかの脅威からスタンドアロンシステムを守ることも依然として重要である。スタンドアロンシステムは、一般にネットワークサービスへの攻撃や悪意のあるペイロード（ウイルスやワーム）の脅威にさらされている。これらの攻撃は、可用性に影響する可能性が高いが（システムのクラッシュ、ネットワーク帯域幅全体の消費、機能の破壊などにより）、完全性に影響したり（データファイルのウイルス感染などにより）、機密性に影響したりする（秘匿性の高いデータへのリモートアクセスの提供、電子メールによるデータファイルの他人への転送などにより）こともある。

スタンドアロン環境のベースラインとなる技術的セキュリティ活動には、一般的な初期設定の脆弱性からITシステムおよび製品を保護すること、ネットワークへの外部アクセスをブロックすること、可能であればローカルアクセスを制限することなどが含まれる。安価なハードウェアベースのファイアウォールルータやパーソナルファイアウォールの導入が、スタンドアロン環境のセキュリティ強化に役立つ場合もある。スタンドアロンのセキュリティのもう 1 つの鍵は、脆弱性に対してパッチを適用し、不要なサービスやアプリケーションを制限するように設定を変更することによって、スタンドアロンネットワーク上のホストのセキュリティを強化することである。スタンドアロン環境に関して一般的に受け入れられているセキュリティ活動の例を次に示す。

- 小規模なハードウェアファイアウォールアプライアンスをインターネット接続部分に使用して、受信接続をブロックし、場合によっては送信トラフィックもフィルタリングする。
- スタンドアロンシステム上でパーソナルファイアウォール製品を使用する。
- アプリケーション（ウイルス対策ソフトウェア、Web ブラウザ、電子メールクライアント）およびオペレーティングシステムの更新やパッチを定期的に適用する。
- 悪意のある内容を含むトラフィックやメッセージをフィルタリングするように Web クライアントと電子メールクライアントを設定する。
- 不要なアプリケーション（パーソナル Web サーバ、SNMP、メッセージングなど）を無効にする。
- ワイヤレスネットワークのトラフィックや（必要に応じて）そのほかのトラフィックに対して暗号化を使用する。
- 有線 LAN または無線 LAN に接続できるシステム／ユーザを制限する。
- ユーザの権限を制限する。
- ディレクトリやプリンタなどのリソースの共有を制限する。
- バックアップと復旧の手順を規定する。
- 物理的セキュリティの手順を規定する。

スタンドアロン環境に関連するセキュリティ活動の詳細な手引きについては、NIST およびそのほかのセキュリティ文書を参照されたい。利用者によっては、Microsoft Windows®システムのシステム管理に関する手引き[13]、[26]、在宅勤務に関する手引き[14]、ワイヤレスネットワークのセキュリティに関する手引き[15]などが特に役立つ場合がある。NIST のコンピュータセキュリティ Web サイト[6]には、さまざまなセキュリティ関連の Special Publication と一般的なセキュリティの手引きが用意されている。

## 3.3 マネージド環境

**マネージド環境は、エンタープライズ環境とも呼ばれ、一般にファイアウォールによってインターネットからの直接のアクセスから保護されている、集中管理された IT 製品のネットワークを表す。図 3-2 に、典型的なエンタープライズネットワークアーキテクチャを示す。この例では、ネットワーク接続されたプリンタと多機能機器、マネージドワークステーション、および内部サーバが含まれる。**

**マネージド環境の利用者には、一般に、中堅～大企業、大規模な政府機関、および管理された在宅勤務システムやリモートオフィスを必要とする組織が含まれる。マネージド環境用チェックリストは、一般に、中～大規模組織の上級エンドユーザおよびシステム管理者を対象としている。マネージド環境には、一般に、ユーザのサポートとセキュリティの提供を専門とするグループがある。このような仕組みと熟練したスタッフの組み合わせにより、システムの導入や継続的なサポートおよび保守において、より適切なセキュリティ活動を実施できる。一般的なマネージド環境では、管理が行われるという性質上、管理者がワークステーション、サーバ、そのほかの種類の機器に対する各種の設定、およびリソース（ファイルサーバ、プリンタなど）の共有を集中的に管理できる。エンタープライズ環境では、通常の業務運営に必要なサービスだけが有効化され、悪用されるおそれのあるそのほかのサービスは削除または無効化される。組織全体で一貫したセキュリティ状況を維持するために、認証管理、アカウント管理、およびポリシー管理を集中的に行うこともできる。**

### 3.3.1 脅威の考察と推奨される技術的セキュリティ活動

**マネージドネットワークに対するリモートおよびローカルの脅威は、システムやアプリケーションに対して大きな影響を与える可能性がある。マネージド組織には、多くの場合、インターネット上で攻撃者が目にする可能性が高い既知の固定 IP アドレスと名前空間を持ったシステムがある。エンタープライズネットワーク上のシステムの多くは、通常、インターネットに直接公開されないようにファイアウォールによって保護された内向きシステムであるが、侵入者は別の手段でこれらのシステムに侵入することによって内部のネットワークにアクセスできることがある。たとえば、ウイルスやワームは短期間のうちに共通の機種で構成されたネットワーク全体に広がる可能性がある。また、マネージド環境では、ユーザの数が多いため、一般にインサイダーによる脅威の方が大きい。**

**マネージド環境は、スタンドアロン環境に比べて制限が強く、提供される機能も少ない。しかし、一般にマネージド環境では、さまざまな種類のトラフィックがより適切に管理される。たとえば、企業と外部ネットワークとの接続部分における、プロトコルとポートに基づいたトラフィックのフィルタリングなどがある。マネージド環境は、サポートされていることと、その大部分が同一の機種で構成されていることから、一般にスタンドアロン環境よりも機能面に制限を加える設定を適用しやすい。また、マネージド環境では、より大きな保護を提供する多重防御（ファイアウォール、ウイルス対策サーバ、侵入検知システム、パッチ管理システム、電子メールフィルタリングなど）を実装する場合が多い。**

[6] NIST のコンピュータセキュリティ Web サイトは、http://csrc.nist.gov/にある。

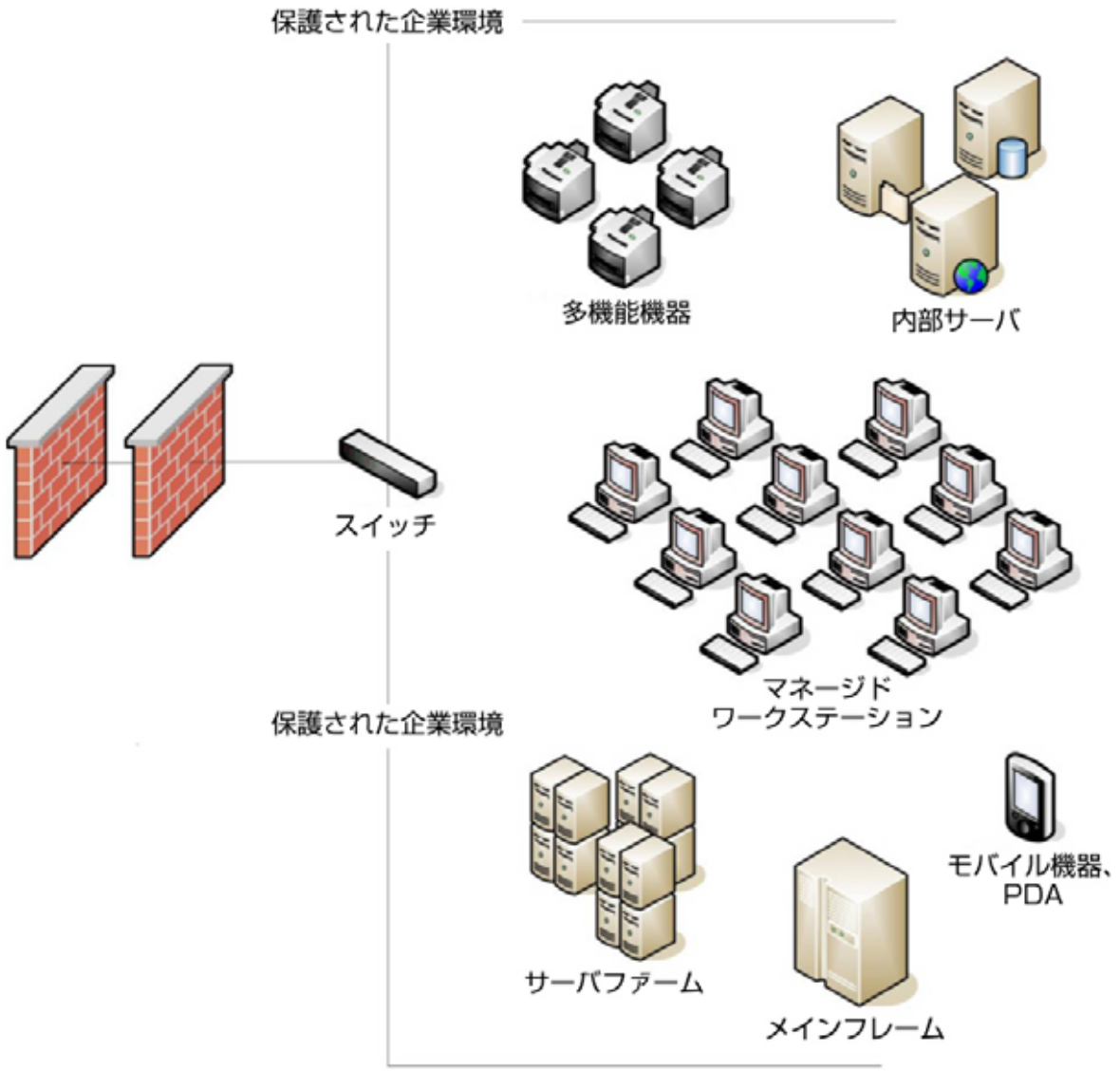


**図 3-2：集中管理されたマネージド環境の例**

マネージド環境のシステムは一般にローカルおよびリモートの脅威の影響を受けやすい。ローカルの攻撃（別ユーザのワークステーションの無断使用など）は、ほとんどの場合、機密性の喪失（データへの無許可アクセスなど）を招くが、完全性（データの改変など）や可用性（システムの盗難など）の喪失を招くこともある。リモートの脅威は、組織外の攻撃者だけでなく、組織のネットワーク内にある他のローカルシステムを攻撃するローカルユーザによってもたらされることもある。リモートの脅威によって生じるほとんどのセキュリティ違反には、部外者によって送信された悪意のあるペイロード（電子メールや、ウイルスに感染した Web サイトを通じて受け取ったウイルスやワームなど）が関与している。ネットワークベースのアプリケーションに対する脅威は、少数のシステムに影響する傾向があり、部内者または部外者によってもたらされる可能性がある。悪意のあるペイロードも、ネットワークアプリケーションへの攻撃も、可用性に影響する可能性が高いが（システムのクラッシュ、ネットワークの全帯域の消費、機能の破壊など）、完全性（データファイルのウイルス感染など）や機密性（秘匿性の高いデータへのリモートアクセスの提供など）に影響することもある。データ漏洩の脅威は、ローカルネットワークのトラフィックを監視している部内者によってもたらされる傾向があり、主に機密性に影響を与える。

マネージド環境に関して一般的に受け入れられているセキュリティ活動の例を次に示す。

- 内部ファイアウォールやそのほかの縦深防御技術によって内部ネットワークをセグメントに分ける。
- システムを集中管理し、ローカルユーザのアクセスを厳しく制限する。
- ウイルス対策などのセキュリティ関連アプリケーションを集中管理する。
- システムおよびアプリケーションのパッチや更新のインストールを自動化する。
- プリンタおよび多機能機器へのアクセスやそれらの機能の使用を制限する。
- ログ監視のシステムを集中化する。
- バックアップと復旧の機能を集中化する。

マネージド環境に関連するセキュリティ活動の詳細な手引きについては、各種のセキュリティ文書を参照されたい。NIST は、マネージド運用環境に特に役立つ各種の SP シリーズ文書を発行している。NIST のセキュリティ Web サイトから入手できる関連刊行物として、Microsoft Windows システムのシステム管理[13]、[26]、ワイヤレスネットワークのセキュリティ[15]、アクティブなコンテンツとモバイルコード[16]、セキュリティパッチ[18]、ファイアウォール[19]、ネットワークセキュリティのテスト[20]、およびインシデント対応[25]に関する手引きがある。

## 3.4 セキュリティを優先することによる機能制限環境

**カスタム**環境は、セキュリティの機能とレベルがほかの環境と一致しないシステムを含む。**セキュリティを優先することによる機能制限**環境は、高度に機能が制限され、セキュリティが確保された典型的なカスタム環境であり、通常は脅威およびそれに対応する影響の度合いが最も高いシステムのために用意されている。このようなシステムの一般的な例として、外向きの Web サーバ、電子メールサーバ、DNS サーバ、そのほかの公的にアクセスされるシステム、ファイアウォールなどがある。また、機密情報を含むコンピュータ（人事記録、医療記録、財務情報の中央リポジトリなど）やきわめて重要な組織的機能（会計、給与処理、航空管制など）を実行するコンピュータも含まれる。これらのシステムは、第三者が悪用の標的にする可能性もあるが、組織内部の信頼されている関係者が標的にする可能性もある。

セキュリティを優先することによる機能制限環境がほかの環境のサブセットになっている場合もある。たとえば、マネージド環境内に組織の機密扱いの従業員データを保持するデスクトップが 3 つある場合、これらはマネージド環境内部の、セキュリティを優先することによる機能制限環境であると考えられる。また、組織の幹部などがモバイルワーカーとして使用するノート型パソコンは、スタンドアロン環境内部のセキュリティを優先することによる機能制限環境である可能性がある。セキュリティを優先することによる機能制限環境が、秘匿度の高いデータを処理する政府のセキュリティ設備などのように、他の環境の外部にある自己完結型の環境である場合もある。

セキュリティを優先することによる機能制限環境用チェックリストは、厳格な技術的セキュリティ活動を実施した場合の影響を理解している熟練のセキュリティ専門家やベテランのシステム管理者を対象としている。ホームユーザや十分なセキュリティの専門知識を持たないそのほかのユーザがセキュリティを優先することによる機能制限環境用チェックリストをシステムに適用しようとすると、多くの場合、システムの機能が不必要に制限され、場合によってはシステムに復旧不能な損害を与える可能性がある。

### 3.4.1 脅威の考察と推奨される技術的セキュリティ活動

この環境内のシステムは、マネージド環境内のシステムと同じ脅威に直面する。部内者による攻撃の脅威も大きな懸念事項であるが、主な攻撃媒介要素は外部からのものである可能性が高い。システムはインターネットに直接接続され、マネージド環境と同じように攻撃者が目にする可能性が高い既知の固定 IP アドレスと名前空間を持っている。自動化された侵入やサービス不能攻撃（DoS）だけでなく、手動による侵入も受けやすい。ファイアウォールやサーバが侵入されると、ローカルの攻撃や侵入につな

がるおそれがある。ローカルの脅威は、システムが多くのユーザを持つ大規模なネットワークに接続されている場合は増大し、小規模なネットワークに接続されている場合は減少する。セキュリティ侵害のリスクと予想される結果に対応するため、通常、この環境は最も機能的な制限の多い、セキュリティの高い設定を持っている。推奨される設定では、使い勝手、機能、およびリモートシステムの管理を大幅に犠牲にした上で、最も高いレベルの保護が提供される。

セキュリティを優先することによる機能制限環境と見なされるシステムやアプリケーションにはさまざまな種類があるため、技術的セキュリティ活動はごく一般的なレベルでしか規定できない。しかし、次の一般的な活動および管理策を適用できる可能性がある。

- 一般に、システムで処理するデータの種類をできるだけ少なくする（たとえば、同じシステムに複数のサーバアプリケーションを統合しない）こと。
- システムから不要なサービスやアプリケーションを取り除くこと。
- 可能であれば、ホストベースのファイアウォールアプリケーションを使用すること。
- システムに必要なだけのユーザしか登録しないこと。
- できるだけ強力な認証機能（認証トークン、生体認証、スマートカードなど）を使用すること。
- リモート管理やリモートアクセスを制限すること。使用する場合は、接続を暗号化すること。
- オペレーティングシステムおよびアプリケーションのセキュリティ関連パッチや更新をできるだけ早くテストし、適用すること。
- アクセスを制限して不要なプロトコルをフィルタリングするファイアウォールやそのほかのネットワークセキュリティ機器の背後にシステムを配置すること。
- 侵入検知やそのほかのログを定期的に監視すること。
- システムに対して定期的に脆弱性評価ツールを実行すること。
- システム管理者は、必要な技術に高いレベルで習熟していること。

NIST およびそのほかの組織は、ファイアウォール[19]、Web サーバ[21]、および電子メール[22]に関するセキュリティ活動を推奨している。推奨事項の詳細については、スタンドアロン環境およびエンタープライズ環境の箇所で示した刊行物を参照されたい。

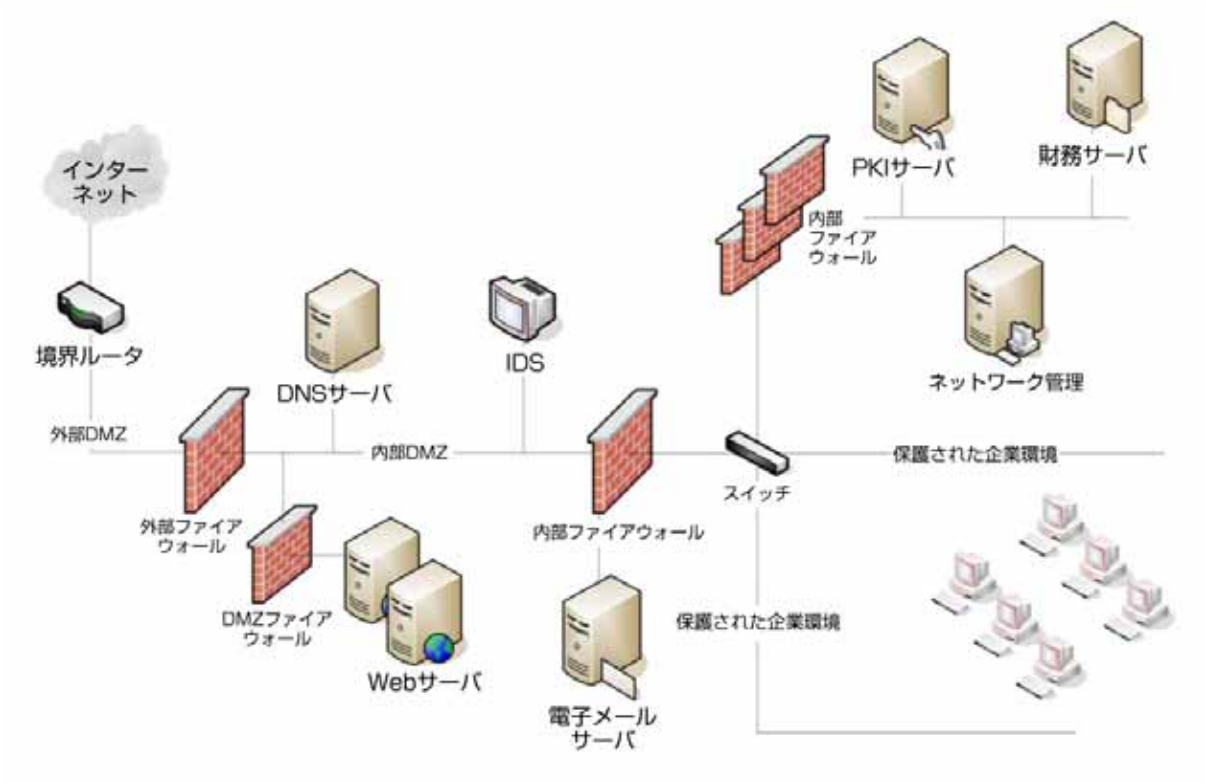


**図 3-3：セキュリティを優先することによる機能制限環境の典型的な例**

## 3.5 レガシー環境

レガシー環境は、カスタム環境のもう 1 つの例である。レガシー環境では、レガシーシステムを新しい設備と組み合わせるとともに、こんにちの脅威に対応するためにセキュリティを確保する必要がある。脅威の考察については、状況に応じて大きく異なる。

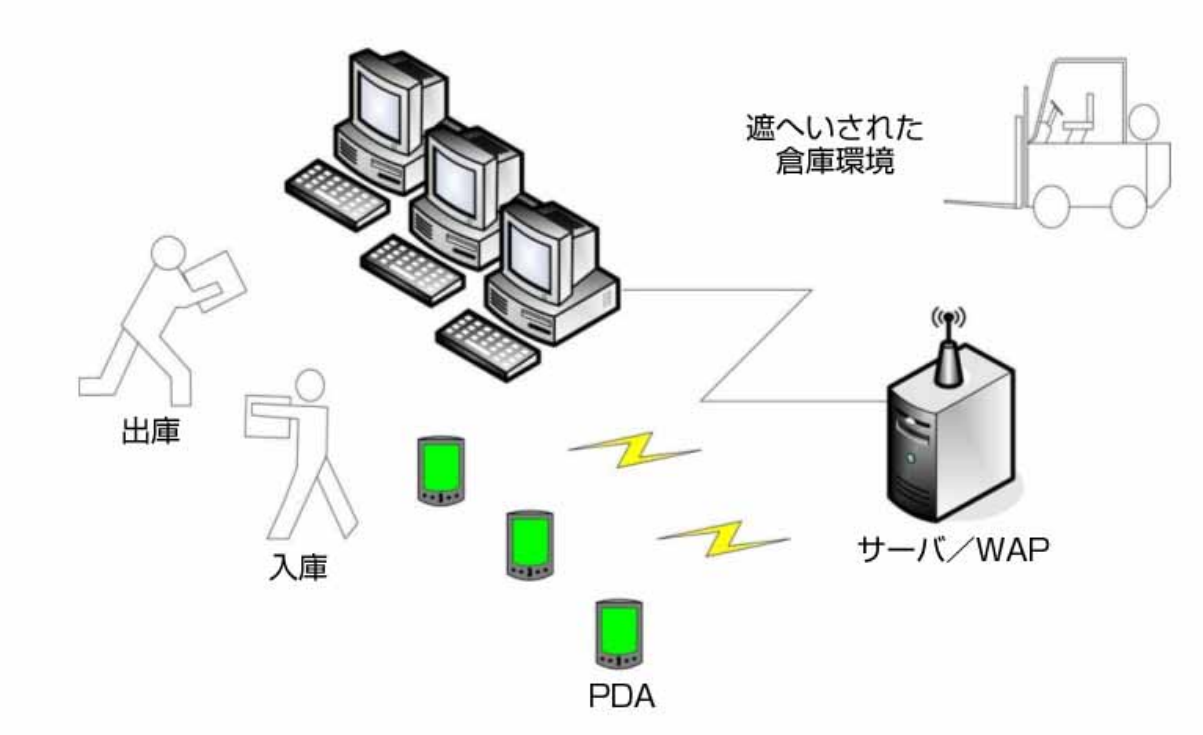


**図 3-4：レガシー環境の例**

レガシー環境の例を図 3-4 に示す。倉庫作業員がワイヤレス PDA 機器を使って出庫と入庫の明細を収集する。PDA をアップグレードして暗号化が可能なワイヤレスプロトコル（WEP や WPA など）をサポートするには、高いコストがかかる。しかし、この倉庫の場所や構造により、ワイヤレストラフィックが簡単には傍受できないようになっている。コストを考慮してリスクの判定が行われ、サーバ／ワイヤレスアクセスポイントのためのレガシー環境チェックリストが作成された。

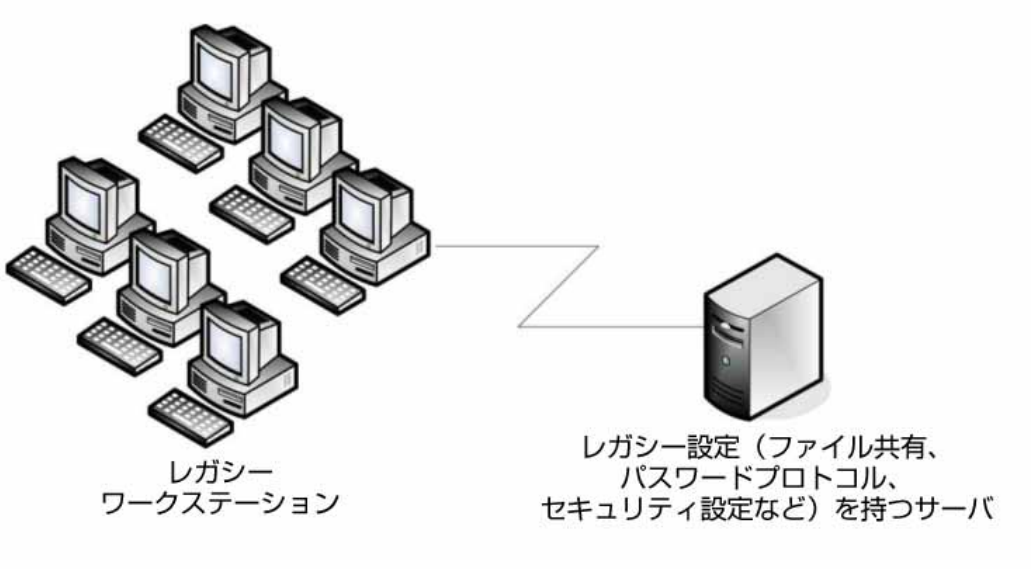


**図 3-5：レガシーワークステーション環境**

図 3-5 にレガシー環境のもう 1 つの簡単な例を示す。この例では、最近のサーバ技術を使用するネットワークに旧型のワークステーションを組み込む必要がある。旧型のワークステーションは、最近の技術

が持つ新しい堅牢な機能（セキュリティが強化されたファイル共有プロトコル、ファイルシステム、認証プロトコルなど）をサポートできない。このため、レガシーワークステーションをサポートするには何らかの変更を行う必要がある。この例では、サーバにレガシー環境チェックリストが必要である。

# 4. チェックリストの使用

このセクションでは、チェックリスト利用者がチェックリストを入手して使用するときに従うべきプロセスの概要を説明する。家庭のユーザから大規模組織のシステム管理者に至る、どのチェックリスト利用者にもそれぞれ固有の要求事項があるが、ここで説明するプロセスはほとんどの状況に当てはまる。このセクションには、ローカル環境の脅威とリスク、および脅威が発生した場合の影響について初期の分析を実施するための手引きが含まれる。次に、NIST チェックリストリポジトリからチェックリストを選択して入手するためのプロセスを説明し、チェックリストの分析、調整、適用の手順を推奨する。

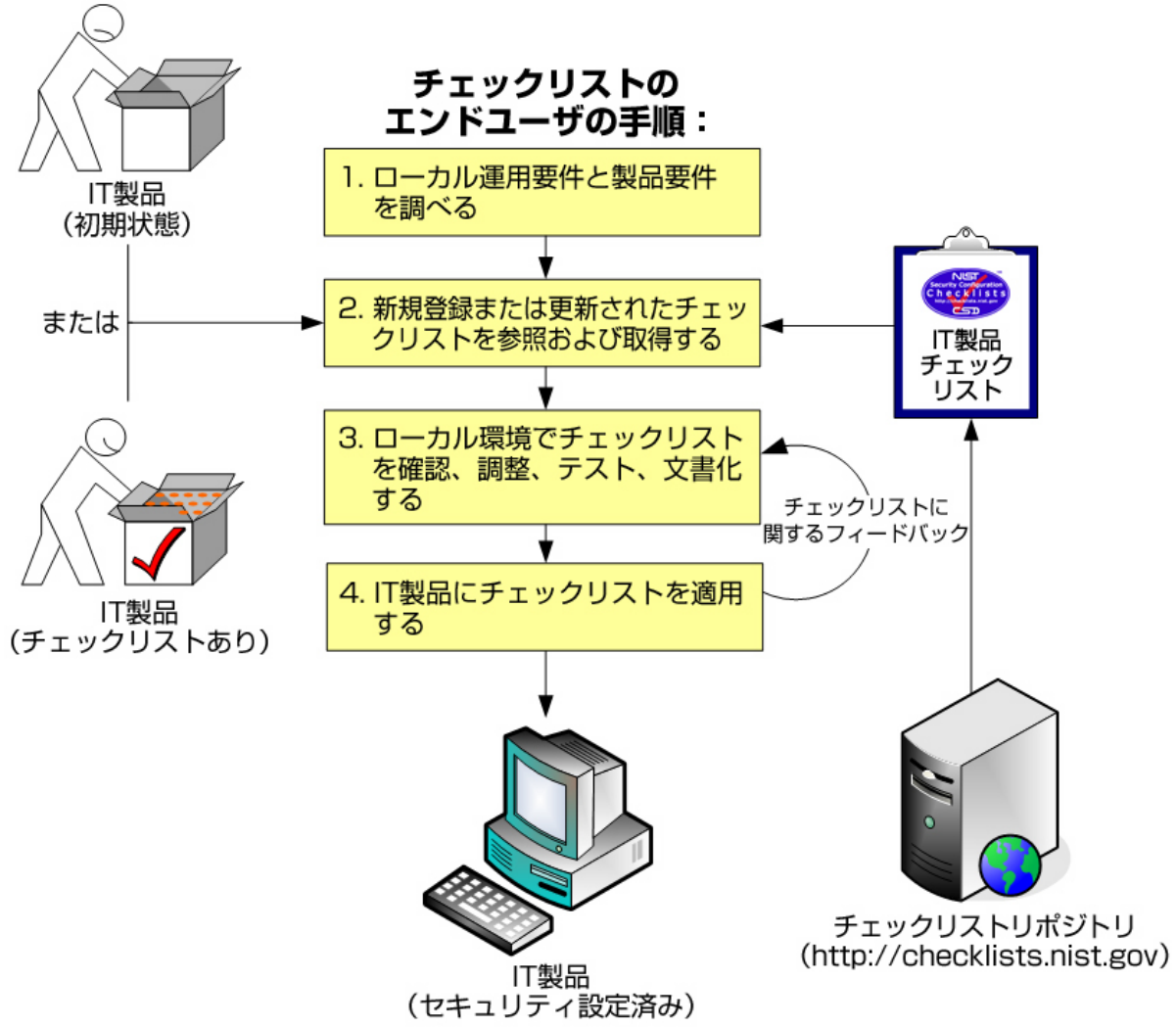


**図 4-1：チェックリスト利用者のプロセスの概要**

図 4-1 に、チェックリストを使用するための一般的なプロセスを示す。手順 1 で、チェックリストの利用を考えている利用者はローカルな要求事項とセキュリティニーズまたはセキュリティポリシーを分析し、適切な運用環境モデルを特定する。次に、利用者はニーズに最も合った IT 製品を選択する。手順 2 で、利用者は IT 製品および選択した運用環境（そして、場合によってはチェックリストをロールバックできるかどうか、製品ベンダーがチェックリストをサポートしているかどうかなどの他の基準）に一致するチェックリストをリポジトリで参照する。利用者は、付属する文書やツールとともにチェックリストをダウンロードする。手順 3 で、利用者はダウンロードしたチェックリストの確認とテストを行い、必要な場合はローカルのポリシーや機能に合わせてチェックリストをカスタマイズする。チェックリストに対するフィードバックは、リポジトリを介して NIST や開発者に送信できる。手順 4 で、利用者はチェックリストの適用に失敗したり、

チェックリストの適用によって予期しない問題が発生したりした場合に影響を受けるおそれがある情報をバックアップすることにより、チェックリストを実運用システムに適用するための準備を行う。最後に、チェックリストを実運用システムに適用する。以降の各項では、これらの手順をそれぞれ詳しく説明する。

## 4.1 ローカルな要求事項の特定

各組織は、通常、特定の IT 製品を実際に選択または購入する前に要件分析を実施する。この分析では、たとえば、組織のニーズ（製品が何をしなければならないか）や製品のセキュリティ要求事項（関連するセキュリティポリシーなど）を明らかにする。個々のエンドユーザも、同じプロセスを（かなり略式になる場合もあるが）実施できる。セキュリティをあとで追加するのは難しいため、事前に要求事項を評価することは（規模の大小を問わず）IT の運用にセキュリティを組み込むための適切な方法である。

NIST Special Publication 800-30『*IT システムのためのリスクマネジメントガイド（Risk Management Guide for Information Technology Systems）*』[12]には、連邦政府機関が要件分析とそれに続くリスクアセスメントを実施する際の有益な手引きが記載されている。各組織は、リスクアセスメントを使って、潜在的脅威の程度と IT システムまたは製品のライフサイクル全体に関連するリスクを特定する。このプロセスの結果は、リスクを低減または解消するための適切な管理策を明らかにするのに役立つ（リスクとは、ある脅威源が特定の潜在的な脆弱性を悪用する可能性とその有害な事象が組織に及ぼす影響からなる関数である）。連邦政府機関以外の組織も、SP 800-30 の方法論に従うことでメリットが得られる。

この方法論に含まれる手順は、IT セキュリティにそれほど精通していない個人的なホームユーザにとってもごく簡単なものである。重要な手順として、次のようなものがある。

- **機能的ニーズの特定。**製品が何をしなければならないか。適切なセキュリティソリューションを実装しながら機能面の要求事項も満たせる適切なセキュリティ管理策を選択できるようにするには、エンドユーザの要件（たとえば、在宅勤務者向けリモートアクセスや従業員が内部の情報を利用できるようにするための Web サーバなど）を事前に明らかにすることが必要である。
- **脅威と脆弱性の特定。***脅威*とは、ある脅威源が特定の脆弱性を悪用する可能性である。*脆弱性*とは、偶発的に誘発されるか、故意に悪用される可能性がある弱点である。この手順の目標は、検討中の IT 製品またはシステムに当てはまる潜在的脅威源と、その潜在的脅威源によって悪用される可能性がある脆弱性を特定することである。
- **セキュリティニーズの特定。**この手順の目標は、ある脅威によって製品やシステムの脆弱性が悪用される可能性（確率）を最小限に抑えたり解消したりするのに必要な管理策を明らかにすることである。これにより、「製品はどのようなセキュリティ機能を提供しなければならないか」という問いに対する答えが得られる。この情報を得ることにより、各組織はそれぞれのニーズに最も合った IT 製品をより適切に選択できる。

連邦政府機関は、SP 800-30 に示されている正式な要件分析とリスクアセスメントを実施する。どのような組織または個人でも、脅威と脆弱性、および推奨されるセキュリティポリシーを特定する際には、セクション 3 に示した各運用環境に関連する脅威の考察と一般的なセキュリティ活動が役に立つ。たとえば、ホームユーザが製品を購入する場合は（ホームユーザの環境がスタンドアロン環境に適合すると仮定すれば）、事前にセクション 3 のスタンドアロン運用環境に関する考察を検討することができる。ホームユーザは、各自の要件と入手すべき製品の種類を把握していれば、スタンドアロン環境のセキュリティモデルと一般的な推奨事項を使用することにより、ニーズに最も一致する製品を十分な情報に基づいて選択できる。

NIST は、連邦政府機関が情報セキュリティ製品を選択するときや、テスト済み／評価済みの製品を入手して使用するときに役立つ文書や手引きもいくつか作成している[10]、[17]。IT 製品の脆弱性に関

連する情報を特定するために NIST が用意しているもう 1 つの主要な情報源は、ICAT ツールである[7]。このツールは、特定されたシステムの脆弱性とそれらの脆弱性を修正するために用意されたパッチに関する情報への索引を製品ごとに提供する。

## 4.2 チェックリストの参照と入手

チェックリスト利用者は、ローカルな要求事項を明らかにし IT 製品を特定したら、NIST チェックリストリポジトリを参照する準備が整う。図 4-2 に、リポジトリのホームページの例を示す。チェックリストは、主な IT 製品の分類ごと、IT 製品のメーカーごと、およびチェックリストを作成した提出元組織ごとに参照できる。


**図 4-2：NIST チェックリストリポジトリのホームページ**

特定のチェックリストを選択すると、利用者がそれぞれの具体的な目的に合うチェックリストを判定する手立てとなる情報を豊富に含んだ明細のテンプレートが表示される（各チェックリストの明細に使われるすべてのフィールドの一覧と定義は、付録 B にある）。利用者のニーズ、役割、スキル（ホームユーザ、企業の管理者など）に応じて、明細に含まれる各フィールドの重要性は異なる。表 4-1 に、すべての利用者がそれぞれの具体的なニーズに合ったチェックリストを判定するのに役立つフィールドの一覧を示す。

[7] ICAT ツールは http://icat.nist.gov/にある。

表 4-1：チェックリストの明細フィールド

| フィールド名 | 内容 |
|---|---|
| Checklist Summary（チェックリストの要約） | チェックリストの目的とその設定の要約を示す。 |
| Status（状態） | Candidate（候補）、Final（最終）、Archived（アーカイブ済み）のいずれか。このフィールドは NIST が記入する。 |
| Version（バージョン） | チェックリストのバージョン番号またはリリース番号を示す。 |
| Comments, Warnings, Disclaimer, Miscellaneous（コメント、警告、免責事項、そのほか） | チェックリスト開発者が利用者に伝えたい追加情報。 |
| Revision Date（改訂日） | チェックリストの最新改訂日を CCYY-MM-DD 形式で示す。このフィールドは NIST が記入する。 |
| Vendor（ベンダー） | 対象 IT 製品のメーカー名を示す。 |
| Point of Contact（連絡窓口） | チェックリストに関連した質問、コメント、提案、問題レポートの送信先となる電子メールアドレスを示す。連絡窓口には、チェックリスト開発者がチェックリストの問題レポートの受信を監視している電子メールアドレスが指定されているはずである。 |
| Product Category（製品の分類） | IT 製品の主要製品分類（ファイアウォール、IDS、オペレーティングシステム、Web サーバなど）。 |
| Product（製品） | IT 製品の正式名称。 |
| Product Role（製品の役割） | チェックリストに記述された IT 製品の主な用途や機能（クライアントデスクトップホスト、Web サーバ、要塞ホスト、ネットワーク境界保護、侵入検知など）を示す。 |
| Product Version（製品バージョン） | IT 製品の特定のソフトウェアまたはファームウェアのリリースバージョン番号（必要に応じて、サービスパックやパッチレベルを含む）。 |
| Rollback Capability（ロールバック機能） | チェックリストの適用によって変更された製品の設定をロールバックできるかどうか、またできる場合は、変更をロールバックする方法を示す。 |
| Submitting Organization/Authors（提出組織／作成者） | チェックリストを作成した組織または作成者の名前。 |
| Target Audience（対象となる利用者） | チェックリストを導入、テスト、使用できる対象利用者（チェックリストを正しく使用するために必要な推奨される最低限のスキルや知識を含む） |
| Target Operational Environment（対象となる運用環境） | IT 製品の運用環境。たとえば、スタンドアロン（Standalone）、マネージド（Managed）、カスタム（Custom）（セキュリティを優先することによる機能制限（Specialized Security-Limited Functionality）やレガシー（Legacy）などの詳細を含む）など。 |
| Testing Information（テスト情報） | チェックリストのテストが行われたプラットフォーム。追加的なテスト関連情報（使用したテスト手順の要約など）を含むこともある。 |
| Product Support（製品サポート） | ベンダーは、このチェックリストを IT 製品に適用した利用者からのサポート電話を受け付ける。IT 製品の保証には影響を与えない。チェックリストプログラムのロゴを使用する場合に必要。 |

## 4.3 チェックリストの確認、カスタマイズ、文書化、およびテスト

チェックリスト利用者は、チェックリストに関するすべての文書をダウンロードし、それらを入念に確認するべきである。これらの文書では、事前に行う必要がある活動（システムのバックアップなど）が説明されている。チェックリストが利用者固有の要求事項に完全に一致することはないため、この確認作業は、チェックリストを変更する必要があるかどうか、チェックリスト適用後のシステムまたは製品に対して追加的な変更が必要かどうかなどを判定するのに役立つ。

大規模な組織では、この確認作業によって、特定のセキュリティチェックリストを適用した場合の現行のポリシーや活動に対する影響を明らかにできる（たとえば、ブラウザの JavaScript を無効にするチェックリストを適用すると、一部の Web ページが使用できなくなる可能性がある）。組織によっては、チェックリストの一部が組織固有の特定のニーズや要求事項に適合しないと判断する場合もある。各組織は、ローカルの規則、規制、義務が反映されるようにチェックリストを調整するべきである。チェックリストは組織内で繰り返し適用される可能性があるため、場合によってはチェックリスト自体を変更する必要がある。これは特に、システムに適用されるスクリプトやテンプレートがチェックリストに含まれている場合に可能性が高い。

この時点で、チェックリストに対する変更がある場合は、今後のためにそれを文書化するべきである。また、フィードバックを NIST およびチェックリスト開発者に送付することができる。フィードバックは、チェックリストのでき具合や対象となる環境に対して設定を適用できるかどうかを開発者が判断する上で特に重要である。

利用者は、チェックリストを適用する前にまず重要でないシステム（できれば管理された非運用環境）を使ってチェックリストをテストするべきである（ただし、テスト用の予備のシステムやネットワークを持たないホームユーザや小規模企業ユーザにとっては、テストの実施が困難な場合もある）。IT 製品のテスト用設定は、導入時の設定と同じにするべきである。場合によっては、セキュリティ管理策の変更によって、製品の機能や使い勝手に対して、またはほかの製品やセキュリティ管理策に対してマイナスの影響が出る可能性がある。たとえば、パッチをインストールすることでほかのパッチが意図せず破損したり、ファイアウォールを有効にすることでウイルス対策ソフトウェアのシグニチャの更新がブロックされたりパッチ管理ソフトウェアの処理が妨げられたりすることがある。このため、テストを実行することにより、システムのセキュリティ、機能、使い勝手に対する影響を判定し、重大な問題を解決するために適切な措置を講じることが重要である。4.4 項では、バックアップ実行時の推奨事項と、テストしていないチェックリストを適用した場合に発生するおそれがある潜在的な損害や好ましくない影響を避けるまたは発生した場合にそこから復旧するためのそのほかの提案事項を示す。

## 4.4 IT 製品へのチェックリストの適用

各チェックリストには、導入に役立つ具体的なインストール手順が含まれる。確認とテストが終わっても、セキュリティチェックリストの適用によって生じる可能性がある問題を最小限に抑えるため、利用者は慎重に導入を行うべきである。

非運用環境でチェックリストをテストできない利用者（ホームユーザなど）にとっては、チェックリストのすべての文書を慎重に確認し、事前のバックアップが必須なのか、それとも考慮したほうが良い事なのかを判断することがいっそう重要である。チェックリストの説明に含まれる「*Rollback Capability*」フィールド（表 4-1 を参照）は、チェックリストを無効にして製品を元の設定に戻せるかどうかを示す。この内容に関係なく、チェックリストの適用前に IT 製品の設定をバックアップしておくことを強く推奨する。

利用者は、少なくともコンピューティング環境に含まれる重要なデータファイルをすべてバックアップするべきである。可能であれば、チェックリストを適用する前の状態にシステムを復元する必要が生じた場合に備えて、システムの完全なバックアップを行うべきである（実際、これはシステムに大幅な変更を加える前に行うことが推奨される活動であり、チェックリストの適用に限定されるものではない）。また、大規模な組織では、この手順に従うとともに、可能であれば最初に複数の運用システムを試験用として選択し、エンタープライズレベルの導入前に「実際の状況に沿った」チェックリストのテストを行うべきである。

製品によってはチェックリストが定期的または頻繁に更新されるため、NIST は一部のチェックリストのメール配信用アドレスを管理することがある。アドレスを登録した利用者は、チェックリストに関連する更新やそのほかの問題を通知するメールを受信する。登録手順は、チェックリストリポジトリで選択したチェックリストの説明のなかに記載されている。

NIST は、チェックリスト利用者から送られる個々のチェックリストやリポジトリ全体に関するフィードバック、バグ報告、コメント、提案などをすべて歓迎する。NIST は、開発者がチェックリストの有効性と妥当性をより適切に判断できるように、必要に応じてチェックリスト利用者からのフィードバックを奨励する。

# 5. チェックリストの開発

このセクションでは、セキュリティ設定チェックリストの開発と NIST チェックリストプログラムへの提出の一般的なプロセスを説明する。このなかには、NIST が提出されたチェックリストを検査してリポジトリに公開する際に実行するプロセスの概要や、NIST および開発者がいずれ行われるチェックリストの更新やアーカイブの際に実行するプロセスの概要が含まれる。NIST にチェックリストを提出したい個々の開発者および組織は、この文書の付録に記載されている NIST チェックリストプログラムの管理上の要求事項を確認するべきである。開発者は、チェックリストを NIST に提出する前にこの文書の最新版を持っているかどうかを確認するべきである。最新版は、http://checklists.nist.gov/から独立したファイルとして入手できる。

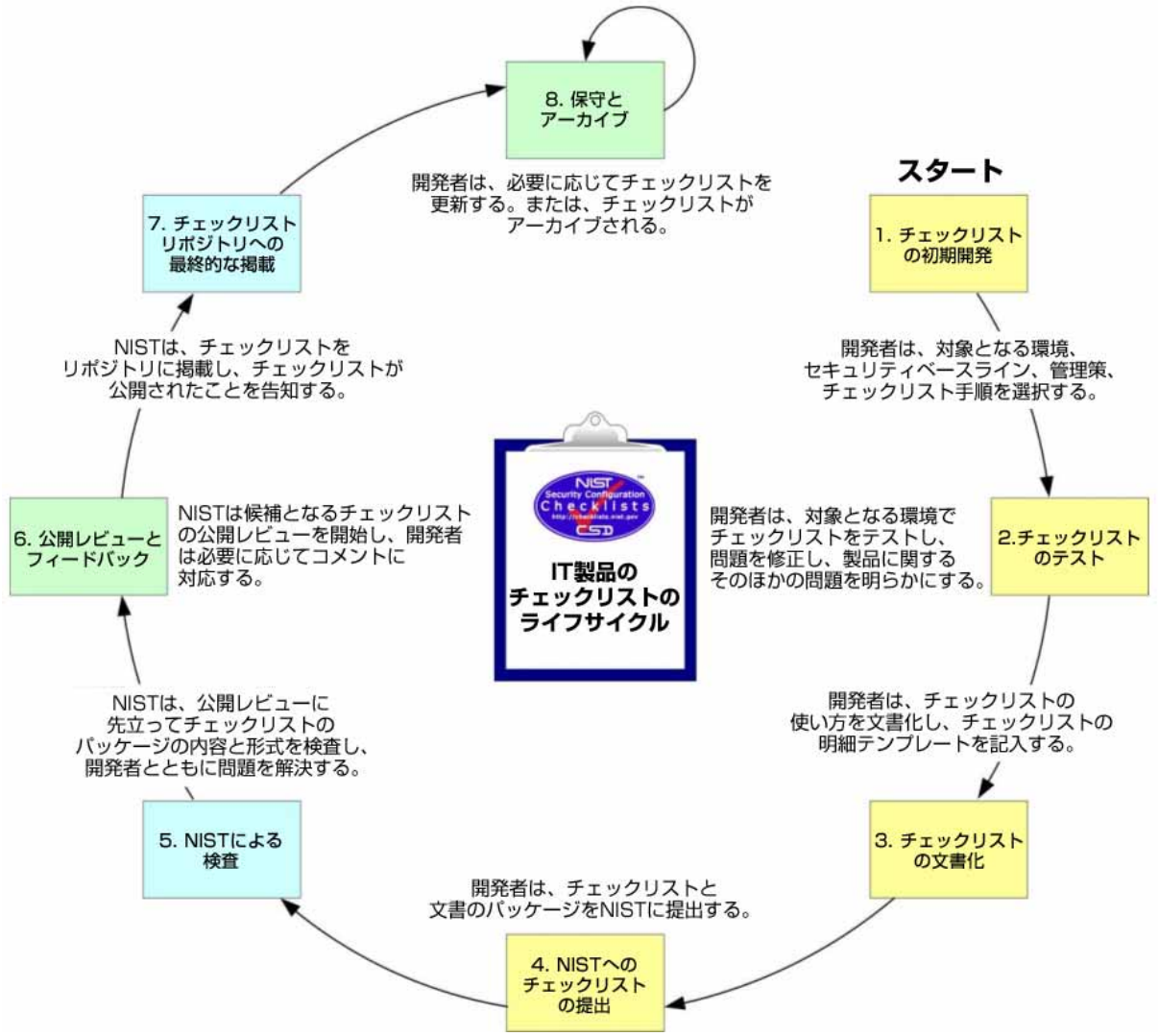


**図 5-1：NIST チェックリストプログラムの開発手順**

図 5-1 に示したライフサイクル手順は単純なものである。チェックリストの開発とその後の公開、更新、アーカイブの過程において、チェックリストを正確なものにし、テストし、文書化するために、これらの手順に従うべきである。以降の各項では、各手順について考慮すべき事項を説明する。

## 5.1 チェックリストに関するセキュリティ関連の基準の背景

このセクションでは、チェックリストにおける技術的セキュリティポリシーおよび活動の一貫性を高めるために NIST が開発者に従うことを推奨するセキュリティ関連の基準を説明する。NIST は、この文書ではチェックリスト開発の詳細を幅広く取り上げることができないと認識している。このため、NIST は NIST Special Publication 800-53[23]、そのほかの NIST 刊行物[8]、[10]、およびそのほかの文献[32]に掲載されている、一般的に受け入れられている技術的セキュリティの原則と活動に基づいてセキュリティ関連の基準を規定した。そのほかに考慮すべき事項については、NIST SP 800-27『*Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*』[11]に掲載されている。安全な情報システムの設計を支援するため、NIST はこの文書で説明するシステムセキュリティに関して、一連のエンジニアリングの原則をまとめた。これらの原則は、IT セキュリティ機能の設計、開発、実装に対する一貫性のある構造化されたアプローチを構成するための基礎になる。SP 800-27 の手引きは、部分的に『*Information Assurance Technical Framework（IATF）*』[32]に基づいている。

チェックリストは、セクション 3 で説明した一般的な運用環境のいずれか（カスタム環境を除く）に一致させる必要がある。そのためには、セクション 3 に示した手引き、このセクションおよび付録 C に示すチェックリストの形式と内容、およびそのほかの一般的に推奨される活動および手順を参考にする必要がある。製品または製品のクラスに対して推奨される活動の手引きがまだ用意されていない場合は、一般的に推奨されるセキュリティ活動（多重防御と多層セキュリティ、最小特権、機密性、完全性、可用性の管理策など）を使用するべきである。

脆弱性の対応範囲の観点から、セキュリティ目標は、最新の脆弱性を考慮に入れ、脆弱性関連情報の公認されたソース（DHS US-CERT、CERT/CC、NIST の ICAT など）と一致させるべきである[8]。セキュリティ目標は、公認されたチェックリスト作成組織（NIST [13]、[26]、国家安全保障局（National Security Agency、以下、NSA と称す）[36]、国防情報システム局（Defense Information Systems Agency、以下、DISA と称す）が作成したセキュリティ技術実装ガイド（Security Technical Implementation Guide、以下、STIG と称す）[37]、およびインターネットセキュリティセンター（Center for Internet Security、以下、CIS と称す）のベンチマーク[38]など）とも一致させるべきである[9]。

連邦政府機関で使用される製品のチェックリスト開発者は、FISMA 関連のセキュリティ管理策ベースラインを参考にすることが推奨される。NIST SP 800-53『連邦政府情報システムにおける推奨セキュリティ管理策（*Recommended Security Controls for Federal Information Systems*）』[23]には、セキュリティ管理策の一覧表が記載されている。当該文書では、管理策をグループ化することにより、連邦政府の情報システムのために、FIPS 199 [27]に規定されている低位、中位、高位のそれぞれに対応して 3 つの最低限のベースラインセキュリティ管理策セットを作成している。これは、連邦政府向けのチェックリストの開発者にとって、連邦政府機関が SP 800-53 の該当するセキュリティ管理策に対応するための手助けとなるチェックリストを作成するのに役立つ場合がある。連邦政府の情報システムに採用される IT 製品の開発者は、さまざまな運用環境において、あるいは、FIPS 199 および SP 800-53 に示されている、異なる影響レベルを有する情報システムに対して推奨される構成設定を提供するチェックリストを作成することにより、準拠することが必須の FISMA の要求事項に連邦政府機関が対応することを支援できる。

## 5.2 開発者がチェックリストを作成して提出するための手順

開発の方法論に含まれる最初の 4 つのステップ（図 5-1 を参照。要約を図 5-2 に示す）は、開発者がチェックリストプログラムの手順と要求事項を理解し、チェックリストの初期開発を行うことから始まる。次に、開発者はチェックリストをテストし、必要に応じてチェックリストを調整する。3 つ目のステップでは、プログラムのガイドラインに従ってチェックリストを文書化する。最後に、開発者はチェックリストの提出パッ

[8] DHS US-CERT のサイトは、http://www.us-cert.gov/である。CERT/CC のサイトは、http://www.cert.org/である。ICAT ツールは、http://icat.nist.gov/にある。

[9] NSA のチェックリストは、http://www.nsa.gov/ia/から入手できる。DISA の STIG は、http://iase.disa.mil/stigs/index.html から入手できる。CIS のサイトは、http://www.cisecurity.org/である。

ケージを準備し、検査と公開レビューを受けるためにそれを NIST に提出する。以降の各項では、それぞれのステップに関わるさまざまな考慮事項を説明する。

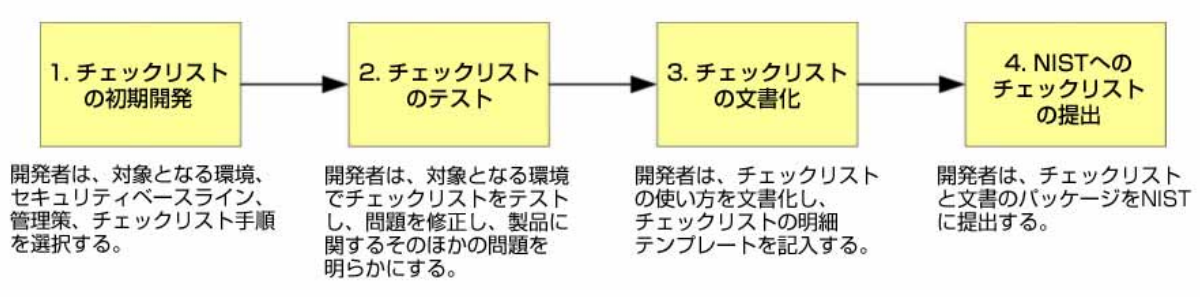


**図 5-2：チェックリスト開発の初期段階**

### 5.2.1 チェックリストの初期開発

この手順において、開発者は（このセクションの全体を通して説明している）チェックリストプログラムの要求事項とチェックリストのライフサイクルにおいて行われるすべての手順を把握する。この時点で、開発者はチェックリストの作成に進む前にプログラム参加のための要求事項に同意しているものと想定されている。プログラムの参加のための要求事項はこの文書の付録 C に記載されているが、管理条項およびプログラム条項として提示されており、技術的な開発者向けというより、開発組織においてプログラムの要求事項に正式に同意する必要がある人を対象として用意されたものである。参加同意書自体は、付録 D に記載されている[10]。

次に、開発者はチェックリストによってセクション 3 のどの運用環境を実装するかを決定し、セクション 3 および 5.1 項に示されたセキュリティ関連の基準を使用して適切なチェックリストを作成する。この手順のアウトプットは、製品の初期チェックリストである。

付録 B に、リポジトリにおけるチェックリスト明細フィールドの完全なセットを示す。利用者は、リポジトリ使用時にこれらのフィールドを検索および参照できる。表 5-1 に、この手順で記入するチェックリスト明細フィールドを示す。

**表 5-1：チェックリストの初期開発時に記入するフィールド**

| フィールド名 | 内容 |
|---|---|
| Vendor（ベンダー） | 対象 IT 製品のメーカー名を示す。 |
| Product Category（製品の分類） | IT 製品の主要製品分類（ファイアウォール、IDS、オペレーティングシステム、Web サーバなど）。 |
| Product（製品） | IT 製品の正式名称。 |
| Product Version（製品バージョン） | IT 製品の特定のソフトウェアまたはファームウェアのリリースバージョン番号（必要に応じて、サービスパックやパッチレベルを含む）。 |
| Target Operational Environment（対象となる運用環境） | IT 製品の運用環境。たとえば、スタンドアロン（Standalone）、マネージド（Managed）、カスタム（Custom）（レガシー（Legacy）やセキュリティを優先することによる機能制限（Specialized Security-Limited Functionality）などの説明を含む）など。 |
| Target Audience（対象となる利用者） | チェックリストを導入、テスト、使用する能力を有する、対象となる利用者（チェックリストを正しく使用するために必要な推奨される最低限のスキルや知識を含む） |

[10] これらのセクションやこの文書の最新版は、http://checklists.nist.gov/から入手できる。プログラムへの参加に正式に同意する前に、これらの更新された資料を参照すること。

| フィールド名 | 内容 |
|---|---|
| Name（名前） | チェックリストの名前を示す。 |
| Checklist Summary（チェックリストの要約） | チェックリストの目的とその設定の要約を示す。 |
| Submitting Organization/Authors（提出組織／作成者） | チェックリストを作成した組織または作成者の名前。 |
| Product Role（製品の役割） | チェックリストに記述された IT 製品の主な用途や機能（クライアントデスクトップホスト、Web サーバ、要塞ホスト、ネットワーク境界保護、侵入検知など）を示す。 |
| Checklist Installation Tools（チェックリストのインストールツール） | チェックリストを使ってシステムを設定するのに必要な機能ツール（チェックリストに付属しない場合）。 |

### 5.2.2 チェックリストのテスト

チェックリストを NIST に提出する前に、対象となる環境およびプラットフォームに適合する設定で、チェックリストを十分にテストするべきである。チェックリストのテストは、さまざまなアプリケーションやハードウェアプラットフォームを使って行うべきである（該当する場合）。テストに使用したデータを NIST に提出する必要はないが、開発者は、必要に応じて確認できるようにテストデータを保管しておくべきである。

表 5-2 に、この手順で記入するチェックリスト明細フィールドを示す。

表 5-2：チェックリストのテスト時に記入するフィールド

| フィールド名 | 内容 |
|---|---|
| Known Issues（既知の問題） | 利用者がチェックリストによって発生する機能上および運用上の問題を特定できるように、チェックリストの適用後に発生する可能性がある問題の要約を示す。 |
| Testing Information（テスト情報） | チェックリストのテストが行われたプラットフォーム。追加的なテスト関連情報（使用したテスト手順の要約など）を含むこともある。 |
| Rollback Capability（ロールバック機能） | チェックリストの適用によって変更された製品の設定をロールバックできるかどうか、またできる場合は、変更をロールバックする方法を示す。 |

セキュリティ管理策の多くは、システムの機能や使い勝手を制限するものであるため、最適なセキュリティ管理策セットの選択は困難な作業になる可能性がある。場合によっては、あるセキュリティ管理策が別のセキュリティ管理策に悪影響を及ぼすこともある。たとえば、パッチをインストールすることでほかのパッチが意図せず破損したり、ファイアウォールを有効にすることでウイルス対策ソフトウェアのシグニチャの更新がブロックされたりパッチ管理ソフトウェアの処理が妨げられたりすることがある。このため、すべてのセキュリティ管理策についてテストを実行することにより、セキュリティ管理策がシステムのセキュリティ、機能、使い勝手に与える影響を判定し、重大な問題を解決するための適切な措置を講じることが重要である。

NIST は、脆弱性や設定上の問題に関してシステムをテストする管理者を支援するため、SP 800-42『ネットワークセキュリティテストにおけるガイドライン（*Guideline on Network Security Testing*）』[20]を作成した。この刊行物は、個々の IT 製品ではなくシステムのテストを中心に扱っているが、チェックリスト開発者にとっても有益である可能性がある。

### 5.2.3 チェックリストの文書化

多くの場合、チェックリスト文書の品質はチェックリストの有効性に大きな違いをもたらす。チェックリスト文書では、簡潔かつ適切で網羅的な操作説明によって、チェックリストのインストール方法を明確に説明するのが望ましい。チェックリストをインストールするのに必要なスキルレベルや対象となる環境についても明示する必要がある。チェックリスト文書では、個々の設定の重要性（製品の機能に関する全ての変更を含む）についても説明する。文書には、チェックリストのインストールに成功したことを確認する手順とともに、チェックリストのアンインストールまたはチェックリストをインストールする前の状態に製品を復元するための手引きも含める。チェックリストの設定をロールバックできない場合もあるため、チェックリスト文書において必要に応じてバックアップやシステム復元などの手順を推奨するべきである。

テストの方法（チェックリストのテスト方法や使用したプラットフォームなど）も文書化する。チェックリスト文書には、エラーが発生したり、チェックリストの設定によって製品が正常に動作しなくなったりした場合のトラブルシューティングの情報も含める。問題が発生した場合に（登録されている）製品ユーザに対して支援を提供できるのが理想である。

表 5-3 に、この手順で記入するチェックリストの追加的な明細フィールドを示す。

**表 5-3：文書化の追加的なフィールド**

| フィールド名 | 内容 |
|---|---|
| Checklist Target Audience（対象となるチェックリスト利用者） | チェックリストを導入、テスト、使用できる対象利用者（チェックリストを正しく使用するために必要な推奨される最低限のスキルや知識を含む） |
| Download Package（ダウンロードパッケージ） | チェックリスト文書の URL またはファイル名。 |
| Checklist Point of Contact（チェックリストの連絡窓口） | チェックリストに関連した質問、コメント、提案、問題レポートの送信先となる電子メールアドレスを示す。連絡窓口には、チェックリスト開発者がチェックリストの問題レポートの受信を監視している電子メールアドレスを指定する。 |
| References（参考資料） | チェックリストまたはチェックリスト文書の作成に使った補助的な参考資料を開発者が選んで示す。 |
| Product Support（製品サポート） | ベンダーは、このチェックリストを IT 製品に適用した利用者からのサポート電話を受け付ける。IT 製品の保証には影響を与えない。チェックリストプログラムのロゴを使用する場合に必要。 |
| NIAP/CMVP Checklist（NIAP／CMVP チェックリスト） | 製品がこのチェックリストを使って NIAP または CMVP の下で評価されたかどうか。このフィールドには、受け取った評価の種類も示す。 |
| Comments, Warnings, Disclaimer, Miscellaneous（コメント、警告、免責事項、そのほか） | チェックリスト開発者が利用者に伝えたい追加情報。 |

開発者は、チェックリストを正確に記述し、チェックリストによって実現される内容について利用者の混乱を減らすために、フィールドを指定の通りに記入する必要がある。

要約すると、優れた構成のチェックリスト文書には、必要に応じて次のものが含まれる。

- 網羅的で正確なチェックリストの明細

- セキュリティ目標の表明（対象となる環境や、チェックリスト適用後の製品の予想される動作を含む）
- 対象となる利用者（エンドユーザやシステム管理者など）およびチェックリストをインストールするのに必要な技術スキルのレベル
- チェックリストの設定の説明（各設定が製品の動作に与える効果や、設定によって有効または無効になる機能を含む）
- チェックリストの適用前に必要な、バックアップ手順やそのほかの初期手順
- 必要に応じて、チェックリストの適用（スクリーンショットや図解付きの手順など）やインストール成功の確認をするための段階的な操作手順
- チェックリストのアンインストール手順（該当する場合）
- トラブルシューティングの操作手順、またはそのほかの情報や参考資料

### 5.2.4 NIST へのチェックリストパッケージの提出

この時点で、チェックリスト開発者はチェックリストの作成、テスト、文書化を完了しており、資料のパッケージを NIST に提出する。パッケージには次のものが含まれる。

- チェックリストと設定のファイル、テンプレート、スクリプトなど
- 記入済みのチェックリスト明細
- チェックリスト文書
- 開発者の連絡窓口を明示するもの
- 署名された参加同意書

参加同意書とそのほかの要求事項の詳細は付録 C に示す。この付録には、該当する NIST の連絡先も記載されている。

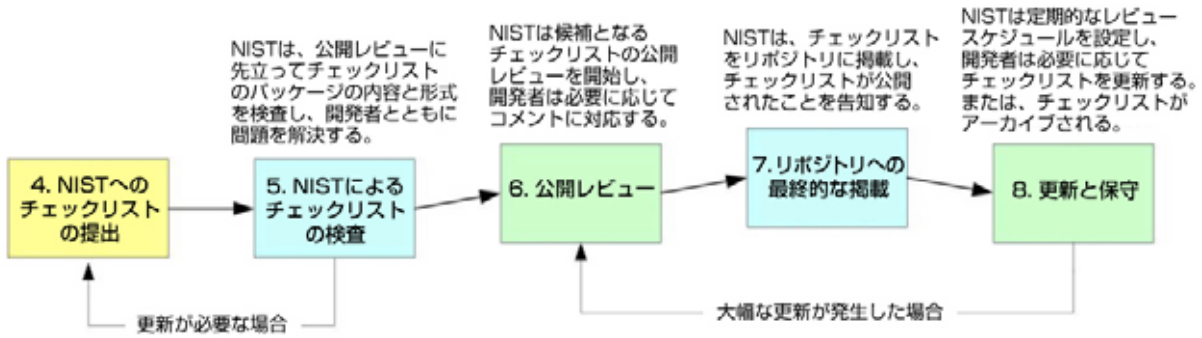


**図 5-3：チェックリストの仕上げと公開の手順**

## 5.3 公開されるチェックリストの NIST による確認と仕上げ

NIST によるチェックリストの検査と公開のプロセスを、以降の各項で説明する。
図 5-3 に、一般的なステップを示す。ステップ 4 および 5 は、開発者へのフィードバックの量に応じて繰り返される場合がある。ステップ 6～8 は、公開済みのチェックリストに対する更新の規模に応じて繰り返される場合がある（大部分の変更については、追加的な公開レビューを行う必要はない）。

### 5.3.1 チェックリストパッケージの検査

このステップでは、チェックリストが公開レビューを受けるのに十分に正確で網羅的であるかどうかが判定される。NIST は、チェックリストの資料を完全性と正確性の点から検査し、チェックリストの評価に使われたテスト手順を調べる。開発者は、検査期間中に提出した資料に関する質問を受けることがある。NIST は、検査を完了し、問題がすべて解決されれば、チェックリストとその明細を通常 30～60 日間にわたって候補として掲載する。

5.1 項で、チェックリストおよびチェックリストの明細の作成に関する基準を示したが、これらの基準はチェックリストの検査にも使われる。基本的に、チェックリストのセキュリティ目標は、NIST やそのほかの公認されたセキュリティ組織が推奨する手引き、およびそのほかのチェックリスト作成組織の手引きに適合するべきである。チェックリストは、このセクションと付録 C に示されたガイドラインに従って文書化されている必要がある。提出されたチェックリストを NIST が検査する際に確認する典型的な項目の例を次に示す。

- 文書
  - 対象となる利用者が規定されているか。
  - 対象となる環境が明示されているか。
  - セキュリティ目標が説明されているか。
  - チェックリストの設定が完全、明確、かつ簡潔に説明されているか。
- ベストプラクティス
  - チェックリストの設定が推奨される活動に合致しているか。
  - チェックリストの設定が最近の脆弱性を考慮に入れているか。
- 設定の影響
  - チェックリスト開発者は、実際的な環境で製品に対するチェックリストの設定をテストし、チェックリストの設定によって製品がチェックリストのセキュリティ目標に適合したことを確認したか。
  - チェックリストのいずれかの設定によって製品が動作不能または不安定にならないか。
  - 特定のチェックリストの設定によって製品の機能が低下しないか。機能が低下する場合、そのことが文書化されているか。
- 実装のしやすさ
  - チェックリストを簡単に適用できるか。
  - 操作手順は、簡潔かつ適切で、完全なものか。
  - 必要なスキルレベルが明示されているか。
  - インストールに成功したことを確認するための手順が記載されているか。
  - チェックリストのアンインストール、またはインストール前の状態に製品を復元するための手引きが記載されているか。
  - チェックリストをロールバックできない場合、バックアップなどの他の事前措置が文書で推奨されているか。
- 支援

- チェックリストに関する支援策が用意されているか。
- エラーが発生したり、チェックリストの設定によって製品が正常に動作しなくなったりした場合のトラブルシューティングの情報が文書に含まれているか。
- 製品の正規ユーザに対する支援が用意されているか。

- チェックリスト開発者が IT 製品のベンダーでない場合、チェックリストが IT 製品のベンダーの支持または承認を受けているかどうかが文書に示されているか。

### 5.3.2 候補となるチェックリストの公開レビュー

チェックリストの検査と開発者による問題解決が完了すると、NIST はチェックリストを公開レビューのために通常 30～60 日間にわたって告示する。これにより、一般の人々がチェックリストの確認とテストを行い、コメントやフィードバックをチェックリスト開発者と NIST に提供できるようになる。これらのコメントやフィードバックは、チェックリストの品質を向上させるために、チェックリストの改訂版に反映できる。候補となるチェックリストのレビュープロセスが完了すると、そのチェックリストはチェックリストリポジトリに追加される。

レビュー者は、標準化されたフィードバックフォームを記入することにより、コメントや、レビュー者のテスト環境、手順、そのほかの関連する情報を記録する。チェックリスト開発者は、レビューの内容によってはコメントに対応する必要がある。NIST が必要に応じて独立の専門レビュー者に助言を求めることもある。独立のレビュー者を利用する一般的な理由の例を次に示す。

- NIST は、コメントへの対応が十分に行われたかどうかを判定するための専門知識が内部にないと判断することがある。
- NIST は、提案された問題解決方法に同意できず、第三者による確認を求めることがある。

公開レビュー期間が終わった時点で、NIST はコメント期間が終了したことを告知する。受け取ったコメントの数とそれらのコメントがチェックリストに及ぼす影響の度合いに応じて、NIST は開発者がコメントに対応するための期間（通常、レビュー期間の終了後 15～30 日間）を決定する。

### 5.3.3 最終的な掲載、保守、およびアーカイブ

重要な問題が解決されたあと、NIST は最終的なチェックリストを掲載し、チェックリストがリポジトリに追加されたことを告知する。開発者（IT 製品ベンダーなど）は、チェックリストに対する支援を行う場合、この時点でチェックリストのロゴを IT 製品の宣伝用資料に使用する資格を得る。ロゴ使用に際しての要求事項は、付録 D に記載されている。

NIST は、残りのライフサイクル全体を通してチェックリストに関する追加のコメントや質問を受け付けるための手順も告知する。製品の種類や更新の発生頻度に応じて、NIST は関連するチェックリストのメール配信用アドレスを管理する場合がある。アドレスを登録した利用者は、チェックリストに関連する更新やそのほかの問題を通知するメールを受信できる。登録手順は、（チェックリストリポジトリの）選択したチェックリストの明細に記載されている。チェックリストのライフサイクル全体を通して、NIST は継続的にフィードバックを収集し、収集した情報をチェックリスト開発者に提供する。

最終的なチェックリストが掲載されると、NIST は開発者とともに定期的なレビュースケジュールを設定する。通常、レビューの間隔は 1 年であるが、特定の要因（新しい脆弱性の発見など）に応じて間隔を縮めることもできる。開発者がチェックリストの更新を決定すると、NIST はチェックリストが更新中であることを告知する。大幅な変更を含むチェックリストは、新しく提出されるチェックリストと同じように扱われ、新しく提出されるチェックリストと同じレビューが行われる。

チェックリストは、開発者の判断でリポジトリから削除されたり、アーカイブの対象として再分類された

りすることがある。一般的な理由としては、製品がサポートされなくなったり古くなったりした場合や、開発者がチェックリストのサポート提供を終了したい場合などが考えられる。

# 付録A. 参考文献

このセクションでは、この文書で使用した参考文献を示す。


[1] Cyber Security Research and Development Act of 2002（2002 年施行のサイバーセキュリティ研究開発法）、http://www.house.gov/science/cyber.htm

[2] Report of the Technical Standards and Common Criteria Task Force、http://www.cyberpartnership.org/init-tech.html

[3] Federal Information Security Management Act (FISMA) of 2002, http://csrc.nist.gov/policies/FISMA-final.pdf

[4] OMB Circular A-130, http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf

[5] Health Insurance Portability and Accountability Act of 1996 (HIPAA), http://aspe.hhs.gov/admnsimp/pl104191.htm

[6] Sarbanes-Oxley Act of 2002, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR:

[7] *The New FISMA Standards and Guidelines*, Ron S. Ross, Ph.D., http://csrc.nist.gov/sec-cert/fisma-article-v15.pdf

[8] NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

[9] NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF

[10] NIST Special Publication 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf

[11] NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security*), http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

[12] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[13] NIST Special Publication 800-43, *Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System*, http://csrc.nist.gov/itsec/guidance_W2Kpro.html

[14] NIST Special Publication 800-46, *Security for Telecommuting and Broadband Communication*, http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf

[15] NIST Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

[16] NIST Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, http://csrc.nist.gov/publications/nistpubs/800-28/sp800-28.pdf

[17] NIST Special Publication 800-36, *Guide to Selecting Information Security Products*, http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

[18] NIST Special Publication 800-40, *Procedures for Handling Security Patches*, http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf

[19] NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

[20] NIST Special Publication 800-42, *Guideline on Network Security Testing*, http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf

[21] NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers*, http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf

[22] NIST Special Publication 800-45, *Guidelines on Electronic Mail Security*, http://csrc.nist.gov/publications/nistpubs/800-45/sp800-45.pdf

[23] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

[24] NIST Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

[25] NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

[26] NIST Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, http://csrc.nist.gov/itsec/guidance_WinXP.html

[27] FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[28] NIST Handbook 150, *Procedures and General Requirements for the National Voluntary Laboratory Accreditation Program*, http://ts.nist.gov/ts/htdocs/210/214/docs/final-hb150-2001.pdf

[29] NIST NVLAP Assessor Declaration, http://ts.nist.gov/ts/htdocs/210/214/assessors/declare.pdf

[30] NIST NVLAP Assessor Performance Information Form, http://ts.nist.gov/ts/htdocs/210/214/assessors/apef.pdf

[31] *Common Criteria for Information Technology Security Evaluation* (CC), Version 2.1, August 1999, http://csrc.nist.gov/cc/CC-v2.1.html

[32] *Information Assurance Technical Framework* (IATF), Release 3.0, October 2000, http://www.iatf.net/, **メンバー専用ページ、サイト登録は** https://www.iatf.net/register/

[33] *Advanced Technology Program Proposal Preparation Kit, Appendix B,* http://www.atp.nist.gov/atp/kit-04/append-b.htm

[34] *ISO/IEC Guide 58*, 1993, available for sale at http://www.iso.ch/iso/en/Standards_Search.StandardsQueryForm

[35] Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC)$^2$ Survey Results, https://www.isc2.org/cgi-bin/index.cgi で登録者が入手可能

[36] National Security Agency (NSA) - Security Configuration Guides, available at http://www.nsa.gov/ia/で入手可能

[37] Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS),https://iase.disa.mil/techguid/stigs.html（.mil ドメインおよび.gov ドメイン用）、http://iase.disa.mil/stigs/index.html（そのほかのドメイン用）

[38] Center for Internet Security (CIS) Benchmarks, http://www.cisecurity.org/で入手可能

[39] National Information Assurance Glossary, CNSS Instruction no. 4009, revised May 2003, http://www.nstissc.gov/Assets/pdf/4009.pdf

（本ページは意図的に白紙のままとする）

# 付録B. チェックリスト明細テンプレート

このセクションでは、チェックリストリポジトリ上のチェックリストごとに維持されるチェックリスト明細のフィールドを示す。記入されたフィールドは、チェックリストに関する情報を利用者に提供するために使われる。

チェックリスト開発者は、チェックリストごとにチェックリスト明細フォームを記入する必要がある。チェックリスト明細フォームの最新バージョンは、チェックリストリポジトリ（http://checklists.nist.gov/）からダウンロードできる。

表 B-1 に、チェックリスト明細のすべてのフィールド（NIST の Microsoft Windows XP チェックリスト[26] のデータが入ったもの）を示す。

**表 B-1：チェックリスト明細テンプレートに含まれるフィールド**

| フィールド名 | 内容 | データ例 |
|---|---|---|
| Name（名前） | チェックリストの名前を示す。 | *SP 800-68: Guidance for Securing Microsoft Windows XP Systems for IT Professionals (Draft)（SP 800-68：IT 担当者のための Microsoft Windows XP システムのセキュリティ確保に関する手引き（草稿））* |
| Version（バージョン） | チェックリストのバージョン番号またはリリース番号を示す。 | *Draft Update R1.0.2（草稿更新 R1.0.2）* |
| Status（状態） | Candidate（候補）、Final（最終）、Archived（アーカイブ済み）、Under Review（レビュー中）のいずれか。 | *Candidate（候補）* |
| Creation Date（作成日） | NIST がチェックリストを最初に掲載した日を CCYY-MM-DD 形式で示す。 | *2004-07-17* |
| Revision Date（改訂日） | チェックリストの最新改訂日を CCYY-MM-DD 形式で示す。 | *2004-08-24* |
| Product Category（製品の分類） | IT 製品の主要製品分類（ファイアウォール、IDS、オペレーティングシステム、Web サーバなど）。 | *Operating System（オペレーティングシステム）* |
| Vendor（ベンダー） | 対象 IT 製品のメーカー名を示す。 | *Microsoft Corporation* |
| Product（製品） | IT 製品の正式名称。 | *Windows XP Professional* |
| Product Version（製品バージョン） | IT 製品の特定のソフトウェアまたはファームウェアのリリースバージョン番号（必要に応じて、サービスパックやパッチレベルを含む）。 | *Microsoft Windows XP 5.1.2600 Service Pack 1 Build 2600* |
| Product Role（製品の役割） | チェックリストに記述された IT 製品の主な用途や機能（クライアントデスクトップホスト、Web サーバ、要塞ホスト、ネットワーク境界保護、侵入検知など）を示す。 | *Client desktop and mobile host（クライアントデスクトップおよびモバイルホスト）* |

| フィールド名 | 内容 | データ例 |
|---|---|---|
| Checklist Summary（チェックリストの要約） | チェックリストの目的とその設定の要約を示す。 | *NIST Special Publication 800-68 has been created to assist IT professionals, in particular Windows XP system administrators and information security personnel, in effectively securing Windows XP systems. It discusses Windows XP and various application security settings in technical detail. The guide provides insight into the threats and security controls that are relevant for various operational environments, such as for a large enterprise or a home office. It describes the need to document, implement, and test security controls, as well as to monitor and maintain systems on an ongoing basis. It presents an overview of the security components offered by Windows XP and provides guidance on installing, backing up, and patching Windows XP systems. It discusses security policy configuration, provides an overview of the settings in the accompanying NIST security templates, and discusses how to apply additional security settings that are not included in the NIST security templates. It demonstrates securing popular office productivity applications, Web browsers, e-mail clients, personal firewalls, antivirus software, and spyware detection and removal utilities on Windows XP systems to provide protection against viruses, worms, Trojan horses, and other types of malicious code. This list is not intended to be a complete list of applications to install on Windows XP system, nor does it imply NIST's endorsement of particular commercial off-the-shelf (COTS) products.*<br>*（NIST Special Publication 800-68 は、IT 担当者（特に Windows XP 管理者および情報セキュリティ担当者）による Windows XP システムの効果的なセキュリティ対策を支援するために作成された。Windows XP と各種アプリケーションのセキュリティ設定に関する技術的詳細を説明する。このガイドから、各種の運用環境（大企業やホームオフィスなど）に関連する脅威とセキュリティ管理策に対する洞察が得られる。セキュリティ管理策の文書化、実装、テストの必要性とともに、継続的なシステムの監視と管理の必要性を示す。Windows XP によって提供されるセキュリティコンポーネントの概要と、Windows XP システムのインストール、バックアップ、パッチ適用に関する手引きを示す。セキュリティポリシー設定を説明し、付属する NIST セキュリティテンプレートの設定の概要を示し、NIST セキュリティテンプレートに含まれない追加的なセキュリティ設定の適用方法を説明する。Windows XP システム上でよく利用されるオフィス生産性向上アプリケーション、Web ブラウザ、電子メールクライアント、パーソナルファイアウォール、ウイルス対策ソフトウェア、およびスパイウェア検出／削除ユーティリティをウイルス、ワーム、トロイの木馬、そのほかの種類の悪意のあるコードから保護するためのセキュリティ対策の実例を示す。このリストは、Windows XP システムにインストールされるアプリケーションの網羅的なリストを意図するものではなく、NIST による特定の民生品の推奨を意味するものでもない。）* |

| フィールド名 | 内容 | データ例 |
|---|---|---|
| Known Issues<br>（既知の問題） | 利用者がチェックリストによって発生する機能上および運用上の問題を特定できるように、チェックリストの適用後に発生する可能性がある問題の要約を示す。 | *Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. These recommendations should be applied only to the Windows XP Systems and will not work on Windows 9X／ME, Windows NT, Windows 2000 or Windows Server 2003. The security templates have been tested on WinXP Professional systems and will not work on Windows 9X／ME, Windows NT, Windows 2000 or Windows Server 2003. The Specialized Security-Limited Functionality template should not be used by home users and should be used with caution since it will restrict the functionality and reduce the usability of the system.*<br>*（このガイドに含まれる設定を実装する場合は、必ず最初に非運用環境で設定をテストすること。これらの推奨設定値は、Windows XP システムのみが適用対象であり、Windows 9X／ME、Windows NT、Windows 2000、Windows Server 2003 には適用できない。セキュリティテンプレートは、Windows XP Professional システムでのみテストされており、Windows 9X／ME、Windows NT、Windows 2000、Windows Server 2003 には適用できない。セキュリティを優先することによる機能制限テンプレートは、ホームユーザが使用するべきでない。このテンプレートは、機能を制限し、システムの使い勝手を低下させるため、慎重に使用する必要がある。）* |
| Target Audience<br>（対象となる利用者） | チェックリストをインストール、テスト、使用できる対象利用者（チェックリストを正しく使用するために必要な推奨される最低限のスキルや知識を含む） | *This checklist has been created for IT professionals, particularly Windows XP system administrators and information security personnel. The document assumes that the reader has experience installing and administering Windows-based systems in domain or standalone configurations.*<br>*（このチェックリストは、IT 担当者（特に Windows XP 管理者および情報セキュリティ担当者）のために作成された。この文書は、ドメイン構成またはスタンドアロン構成に含まれる Windows ベースのシステムをインストールおよび管理した経験がある読者を想定している。）* |
| Target Operational Environment<br>（対象となる運用環境） | IT 製品の運用環境。たとえば、SOHO、エンタープライズ、カスタム（セキュリティを優先することによる機能制限やレガシーなどの記述を含む）など。 | *SOHO, Enterprise, Custom (e.g., Specialized Security-Limited Functionality, Legacy).*<br>*（SOHO、エンタープライズ、カスタム（セキュリティを優先することによる機能制限、レガシーなど）*） |
| Checklist Installation Tools<br>（チェックリストのインストールツール） | チェックリストを使ってシステムを設定するのに必要な機能的ツール（チェックリストに付属しない場合）。 | *The Microsoft Windows tools (e.g., Security Templates MMC snap-in, Security Configuration Analysis MMC snap-in, Group Policy MMC snap-in, Group Policy Management Console MMC snap-in) can be used to customize and apply the NIST security templates to Windows XP systems.*<br>*（NIST セキュリティテンプレートを Windows XP システムに適用するには、Microsoft Windows のツール（セキュリティテンプレート MMC スナップイン、セキュリティの構成と分析 MMC スナップイン、グループポリシースナップイン、グループポリシー管理コンソール MMC スナップインなど）を使用する。）* |

| フィールド名 | 内容 | データ例 |
|---|---|---|
| Rollback Capability<br>（ロールバック機能） | チェックリストの適用によって変更された製品の設定をロールバックできるかどうか、またできる場合は、変更をロールバックする方法を示す。 | *There is no automated way of rolling back the settings unless a full system backup was performed before a security template was applied to the system.*<br>*（設定を自動的にロールバックする方法はない。セキュリティテンプレートをシステムに適用する前に、完全なシステムバックアップを実行すること。）* |
| Testing Information<br>（テスト情報） | チェックリストのテストが行われたプラットフォーム。追加的なテスト関連情報（使用したテスト手順の要約など）を含むこともある。 | *The security templates have been tested on Windows XP Professional systems and will not work on Windows 9X／ME, Windows NT, Windows 2000 or Windows Server 2003. The recommended settings have been tested the suite of applications described in section 8 of NIST SP 800-68.*<br>*（セキュリティテンプレートは、Windows XP Professional システムでのみテストされており、Windows 9X／ME、Windows NT、Windows 2000、Windows Server 2003 には適用できない。推奨設定値は、NIST SP 800-68 のセクション 8 に示した一連のアプリケーションでテストされている。）* |
| NIAP/CMVP Status<br>（NIAP／CMVP ステータス） | 製品がこのチェックリストを使って NIAP または CMVP の下で評価されたかどうか。このフィールドには、受け取った評価の種類も示す。 | *Microsoft Windows XP Professional can be configured to operate in the FIPS validated mode. The product has not been evaluated with a NIAP-approved Common Criteria Testing Laboratory.*<br>*（Microsoft Windows XP Professional は、FIPS で検証されたモードで動作するように設定できる。この製品は、NIAP で承認されたコモンクライテリアのテスト機関では評価されていない。）* |
| Regulatory Compliance<br>（規制の順守） | チェックリストが各種の規制（HIPAA、GLBA、FISMA、ISO17799、米国企業改革法、DoD 8500 など）を順守しているかどうか。 | *The recommendations are consistent with the security control baselines advocated in SP 800-53 draft (NIST FISMA implementation project publication).*<br>*（推奨設定値は、SP 800-53 草稿（NIST の FISMA 実装プロジェクトによる刊行物）で提言されたセキュリティ管理策のベースラインに適合している。）* |
| Comments, Warnings, Disclaimer, Miscellaneous<br>（コメント、警告、免責事項、そのほか） | チェックリスト開発者が利用者に伝えたい追加情報。 | *Refer to Known Issues.*<br>*（「Known Issues（既知の問題）」を参照。）* |
| Disclaimer<br>（免責事項） | チェックリストに関する法的な告知。 | *Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. NIST assumes no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic. NIST would appreciate acknowledgement if the document and template are used.*<br>*（このガイドに含まれる設定を実装する場合は、必ず先に非運用環境で設定をテストすること。NIST は、他の組織によるこのガイドの使用に対していかなる責任も負うものではなく、このガイドの品質、信頼性、またはそのほかの特徴について、明示的にも暗黙的にも保証しない。この文書とテンプレートを使用した場合には、そのことを認知してもらえれば謝意を表する。）* |

| フィールド名 | 内容 | データ例 |
|---|---|---|
| Product Support<br>（製品サポート） | ベンダーは、このチェックリストを IT 製品に適用した利用者からのサポート電話を受け付ける。IT 製品の保証には影響を与えない。 | *Microsoft will provide best efforts support, in line with the customer's support contract, to assist in removing the worst results of such file and registry permissions, but Microsoft can only guarantee returning to the recommended out-of-the-box settings by reformatting and reinstalling the operating system.*<br>*（Microsoft は、このようなファイルやレジストリの許可による最悪の結果を取り除くため、顧客のサポート契約に沿ってベストエフォート方式のサポートを提供する。ただし、Microsoft が保証できるのは、再フォーマットとオペレーティングシステムの再インストールによって、推奨される初期状態の設定に戻すことだけである。）* |
| Submitting Organization/Authors<br>（提出組織／作成者） | チェックリストを作成した組織または作成者の名前。 | *NIST, Computer Security Division*<br>*（NIST、コンピュータセキュリティ部門）* |
| Point of Contact<br>（連絡窓口） | チェックリストに関連した質問、コメント、提案、問題レポートの送信先となる電子メールアドレスを示す。連絡窓口には、チェックリスト開発者がチェックリストの問題レポートの受信を監視している電子メールアドレスを指定する。 | *itsec@nist.gov* |
| Sponsor<br>（スポンサー） | チェックリストが第三者組織によって提出された場合に、提出されたチェックリストを支持する IT 製品の製造組織および個人の名前を示す。 | *Chase Carpenter and Kurt Dillard, Microsoft Corporation* |
| Licensing<br>（ライセンス情報） | ライセンス契約（チェックリストが著作権で保護されている場合や、オープンソース、GPL、フリーソフトウェア、またはシェアウェアである場合など）を示す。 | *This document was developed at the National Institute of Standards and Technology, which collaborated with NSA, DISA, CIS, and Microsoft to produce the Windows XP security templates. Pursuant to title 17 Section 105 of the United States Code this document and template are not subject to copyright protection and are in the public domain.*<br>*（この文書は、米国国立標準技術研究所が Windows XP のセキュリティテンプレートを作成するために NSA、DISA、CIS、および Microsoft と協力して開発したものである。この文書およびテンプレートは、合衆国法典第 17 編第 105 条に記載のとおり、著作権保護の制約を受けず、公共の財産である。）* |
| Checklist Homepage<br>（チェックリストのホームページ） | チェックリストのホームページの URL を示す。 | *http://csrc.nist.gov/itsec/guidance_WinXP.html* |
| Download Package<br>（ダウンロードパッケージ） | チェックリストの文書、スクリプト、テンプレートなどの URL またはファイル名。 | *http://csrc.nist.gov/itsec/guidance_WinXP.html* |
| Integrity（完全性） | チェックリストパッケージのメッセージダイジェストまたはハッシュ。SHA-1 または SHA-256 が推奨される。 | *SHA1 Digest (NIST_WinXP_draft_R1.0.2_08242004.zip) = 9a8f2e8fc7c18e56c9646336c343d1917a2fb02f* |

| フィールド名 | 内容 | データ例 |
|---|---|---|
| Change History<br>（変更履歴） | リポジトリへの追加後に行われたチェックリストの変更の詳細を記録した実行ログ。このフィールドは、チェックリストのバージョンごとに更新される。 | *Security Templates (.inf files)*<br>*（セキュリティテンプレート（.inf ファイル））*<br>*2004-08-24 - Draft Update R1.0.2*<br>*（2004 年 8 月 24 日 - 草稿更新 R1.0.2）*<br>*2004-07-04 - Draft Update R1.0.1*<br>*（2004 年 7 月 4 日 - 草稿更新 R1.0.1）*<br>*2004-06-24 - Draft Release R1.0*<br>*（2004 年 6 月 24 日 - 草稿リリース R1.0）*<br><br>*Draft Guidance for Securing Microsoft Windows XP Systems for IT Professionals document*<br>*（IT 担当者のための Microsoft Windows XP システムのセキュリティ確保に関する手引き（草稿））*<br>*2004-08-24 - Draft Update*<br>*（2004 年 8 月 24 日 - 草稿更新）*<br>*2004-07-04 - Draft Update*<br>*（2004 年 7 月 4 日 - 草稿更新）*<br>*2004-06-24 - Draft Release*<br>*（2004 年 6 月 24 日 - 草稿リリース）* |
| Dependency/Requirement<br>（依存性／要求事項） | 現在のチェックリストを使用および実装するには、別のチェックリストまたはガイドが必要であることを示す。 | *Microsoft Threats and Countermeasures Guide*<br>*（Microsoft の脅威および対抗策に関するガイド）* |
| References<br>（参考文献） | チェックリストまたはチェックリスト文書の作成に使った補助的な参考資料を開発者が選んで示す。 | *DISA, NSA, CIS, Microsoft and other security guides.*<br>*（DISA、NSA、CIS、Microsoft、またはそのほかのセキュリティガイド）* |
| NIST Identifier<br>（NIST 識別子） | チェックリストを一意に識別するために NIST が割り当てた識別子。 | *1001* |

# 付録C. チェックリストプログラムの運用手順

National Institute of Standards and Technology

## IT 製品のための NIST セキュリティ設定チェックリストプログラムの運用手順

バージョン 1.0

この文書は、IT 製品のための NIST セキュリティ設定チェックリストプログラムに関するポリシー、手順、および一般的要求事項を規定したものである。この文書は、開発組織においてプログラムの要求事項に正式に同意する必要がある個人を対象としている。

この文書の構成は次のとおりである。

- セクション 1 - NIST チェックリストプログラムに関する一般考慮事項
- セクション 2 - 公開レビュー前のチェックリストの初期検査手順
- セクション 3 - 候補チェックリストの公開レビュー手順
- セクション 4 - 最終受入手順
- セクション 5 - 保守および掲載終了の手順
- セクション 6 - 記録の保持

この付録では、以下の用語を使用する。

- *候補 (Candidate)*：公開レビューのために NIST が検査し、承認したチェックリスト。
- *FCL*：最終チェックリストの一覧。NIST リポジトリに掲載されるすべての最終チェックリストの一覧のこと。
- *最終 (Final)*：公開レビューが完了し、すべての問題がチェックリスト開発者および NIST によって解決され、このセクションの手順に従ってリポジトリへの掲載が承認されたチェックリスト。
- *チェックリスト (Checklist)*：*技術的設定チェックリスト* (特定の製品およびバージョンに関するチェックリスト)。
- *チェックリスト開発者 (Checklist Developer)* または *開発者 (Developer)*：チェックリストを開発および所有し、それを NIST チェックリストプログラムに提出する個人または組織。

- ***独立公認レビュー者*** *(Independent Qualified Reviewers)*：NIST によって、チェックリストの公開レビューや掲載に関する勧告を NIST に対して行う任務を与えられている。他のレビュー者とは独立に作業を行い、チェックリストによって表される技術の専門家と見なされる。
- ***ロゴ*** *(Logo)*：NIST チェックリストプログラムのロゴ。
- *NIST* ***チェックリストプログラム*** *(NIST Checklist Program)* または ***プログラム*** *(Program)*：IT 製品のための NIST セキュリティ設定チェックリストプログラムと同じ意味で使われる。
- *NIST* ***チェックリストリポジトリ*** *(NIST Checklist Repository)* または ***リポジトリ*** *(Repository)*：チェックリスト、チェックリストの明細、および NIST チェックリストプログラムに関するそのほかの情報を保持する Web サイト。
- ***一般レビュー者*** *(Public Reviewer)*：候補チェックリストを審査し、NIST にコメントを送信する一般市民。
- ***運用環境*** *(Operational Environments)*：この文書で概要を示した運用環境。

**このプログラムの要求事項の基礎になった参照文書を以下に示す。**


- Advanced Technology Program Proposal Preparation Kit Appendix B、http://www.atp.nist.gov/atp/kit-04/append-b.htm
- *Common Criteria for Information Technology Security Evaluation* (CC), Version 2.1, August 1999, http://csrc.nist.gov/cc/CC-v2.1.html
- *Information Assurance Technical Framework* (IATF), Release 3.0, October 2000, http://www.iatf.net/, メンバー専用ページ、サイト登録は https://www.iatf.net/register/
- FIPS PUB 199『Standards for Security Categorization of Federal Information and Information Systems (連邦政府の情報および情報システムに対するセキュリティ分類規格)』、http://csrc.nist.gov/publications/fips/index.html
- NIST Handbook 150, *Procedures and General Requirements for the National Voluntary Laboratory Accreditation Program*, http://ts.nist.gov/ts/htdocs/210/214/docs/final-hb150-2001.pdf
- NIST SP 800-14『*Generally Accepted Principles and Practices for Securing Information Technology Systems*』、http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
- NIST SP 800-27『*Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*』、http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf
- NIST SP 800-53『*Recommended Security Controls for Federal Information Systems (連邦政府情報システムにおける推奨セキュリティ管理策)*』、http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
- NIST SP 800-70『*Security Configuration Checklists Program for IT Products (IT 製品のためのセキュリティ設定チェックリストプログラム)*』、http://csrc.nist.gov/publications/nistpubs/

## 1. 概要と一般考慮事項

このセクションでは、NIST チェックリストプログラムの全体に関する一般考慮事項を中心に扱う。

(a) **チェックリストのライフサイクルの概要**：チェックリストのライフサイクルは、通常、次の通りである。

1. チェックリスト開発者は、プログラムについて問い合わせを行い、提出パッケージをダウンロードする。続いて、開発者は NIST に連絡を取り、テスト済みのチェックリストとサポート情報、および NIST チェックリストプログラムの要求事項への同意書に署名したものを提出する。チェックリストについての一般情報は、セクション 1 に示されている。チェックリスト提出の際の要求事項と手順は、セクション 2 に示されている。
2. NIST は、提出内容に不足がないことを確認し、チェックリストの検査を行う。掲載の要求事項を満たすチェックリストは、検討対象となり、「候補チェックリスト」と呼ばれる。検査の基準と手順は、セクション 2 に示されている。問題解決の手順は、セクション 1d に示されている。
3. NIST は、公開レビューの期間（通常は 30～60 日間）にわたって候補をリポジトリに掲載する（セクション 3 を参照）。
4. NIST は、一般レビュー者からのコメントを開発者に転送する。すべての問題が解決されたチェックリストは、FCL に掲載される（セクション 4 を参照）。
5. 開発者は、通常年 1 回のペースで NIST に連絡を取り、チェックリストの掲載継続、更新、またはアーカイブを決定する（セクション 5 を参照）。

(b) **知的所有権**：開発者は、開発したチェックリストの知的所有権を保持する。

(c) **機密情報**：NIST は、チェックリスト開発者から機密情報を受け取る必要性を想定していない。NIST に機密情報を開示する必要性が生じた場合、NIST と開発者はそのような開示の前に別個の秘密保持契約を結ぶ必要がある。

(d) **独立公認レビュー者**：NIST は、提出されたチェックリストがプログラムの要求事項を満たすかどうかを判断するために、チェックリストを審査する独立の公認された専門家に技術的な助言を求めることがある。これらのレビュー者は、チェックリストのその後の公開レビューや最終的な掲載に関する勧告を NIST に対して行う任務を与えられている。独立のレビュー者を利用する一般的な理由の例を以下に示す（ただし、理由は以下に限定されない）。

1. NIST が、問題への対応が十分に行われたかどうかを判定するための専門知識を持っていない。
2. NIST が、提案された問題解決方法に同意できない。

(e) **提出されたチェックリストの検討の打ち切り**：NIST または開発者は、提出されたチェックリストの検討をいつでも打ち切ることができる。NIST が検討を打ち切る場合は、連絡窓口に対して 10 営業日以内に返答するように求める。提出されたチェックリストの検討を打ち切る一般的な理由を以下に示す（ただし、理由は以下に限定されない）。

1. 提出パッケージが検査基準を満たしていない。
2. 開発者が別の機会に発生した問題を解決できない。
3. 開発者がプログラムの参加条件に違反した。

## 2. チェックリストの提出と検査

このセクションでは、チェックリストを NIST に提出する際の手順と要求事項、およびチェックリストが公開レビューに適しているかどうかを判断する NIST のプロセスを示す。検査基準を満たしているチェックリストは公開レビューの対象となり、「候補チェックリスト」と呼ばれる。NIST は続いて以下の手順を実行する。

(a) **チェックリストプログラム要求事項の通知**：NIST は、開発者向けの情報一式をリポジトリに保持する。これらの情報は、プログラムへの参加に関する要求事項、資料、および期限を示すものである。

(b) **開発者が提出すべき資料**：開発者は、以下の情報をすべて英語で提供する。

1. 提出組織内でチェックリストに関する質問やコメントの連絡窓口を担当する人物の連絡先、および連絡窓口の予備要員または代理担当者の連絡先。これらの情報には、住所、直通電話番号、FAX 番号、および電子メールアドレスを含める必要がある。
2. チェックリスト、文書、および明細テンプレート。
3. 参加同意書（印刷したものに署名し、NIST に送る必要がある）。NIST は、参加同意書のコピーを、電子メールに添付された PDF ファイル、ファックス、または通常郵便で受け取る。
4. 参加費用。現在、チェックリスト開発者は無料で参加できる。NIST は、将来、参加費用を請求する権利を留保する。ただし、過去に遡って費用を請求することはない。

(c) **チェックリスト内容の予備検査**：NIST は、チェックリストがプログラムの要求事項を満たしているかどうかを確認するため、予備検査を行う。以下の項目は、検査基準を要約したもので、詳細は NIST Special Publication 800-70 に記述されている。

1. チェックリストの設定に、推奨されるセキュリティ活動やエンジニアリング活動の考慮事項が反映されている。
2. チェックリストに、構成設定の完全で明確、かつ簡潔な説明が含まれている。
3. チェックリストのテストが完了し、設定や互換性に関する問題が明らかにされている。
4. 文書によって、チェックリストのインストール方法やアンインストール方法が説明されている。
5. チェックリストに関する支援策が用意されている。

## 3. 候補チェックリストの公開レビュー

NIST は、公開レビュー用の候補チェックリストを掲載する際に、以下の手順を実行する。

(a) **公開レビュー期間**：NIST は、コメント期間として候補を通常 30～60 日間にわたって掲載する。NIST は、特に大規模なチェックリストや複雑なチェックリストについて、レビューサイクルを延長する権利を留保する。NIST は、候補チェックリストに関して以下の免責事項（または同様の文言）を使用する。

*NIST は、チェックリストの正確性および完全性を保証しない。NIST は、チェックリストの使用によって発生する可能性がある損失、損害、および問題について責任を負わない。*

(b) **レビュー者からのコメントの受入**：一般レビュー者は、Web ベースのフィードバックフォームを記入することにより、コメントとともに、レビュー者のテスト環境、手順、そのほかの関連する情報を記録する。フィードバックフォームの内容は、公開された記録と見なされる。

(c) **記録の保持**：NIST は、チェックリストごとに固有の電子メールアドレスを作成することにより、一般市民と開発者のあいだで行われるすべてのやり取りとフィードバックのコピーを保持する。NIST は、これらの情報をアーカイブする。

(d) **コメントへの対応**：公開レビュー期間が終わった時点で、NIST はコメント期間が終了したことを告知する。受け取ったコメントの数とそれらのコメントがチェックリストの設定に及ぼす影響の度合いに応じて、NIST は開発者がコメントに対応するための期間を決定する。これは、通常、コメントの提出日またはレビュー期間の終了から 15～30 日間である。この期間が 15 日未満になることはない。

## 4. 最終チェックリストの掲載

NIST は、チェックリストおよび関連する開発者が最終的な掲載の要求事項をすべて満たしていると判断すると、そのチェックリストを FCL に掲載し、「最終チェックリスト」と呼ぶ。NIST は、続いて以下の手順を実行する。

(a) **チェックリストの仕上げ**：NIST は、チェックリストを FCL に掲載する。NIST は、NIST またはそのほかの組織によって管理されている各種のメーリングリストに告知を送信することがある。NIST は、最終チェックリストに関して以下の免責事項（または同様の文言）を使用する。

> *NIST は、チェックリストの正確性および完全性を保証しない。NIST は、チェックリストの使用によって発生する可能性がある損失、損害、および問題について責任を負わない。*

(b) **コメントへの対応**：NIST は、一元的な電子メールアドレスをリポジトリで管理することより、最終チェックリストに関するコメントを継続的に受け入れる。NIST は、開発者の連絡先情報（電子メールアドレスや URL など）とともに開発者への連絡手順を掲載する。

(c) **定期的なレビュースケジュールの設定**：NIST は、最終チェックリストの定期的なレビューを行うかどうかを決定し、レビュー間隔を通常 1 年に設定する。NIST は、新しい脆弱性や脅威の発生を理由に、これよりも早くチェックリストのレビューを求めることがある。NIST は、開発者の連絡窓口とともにレビューのスケジュールを設定する。連絡窓口が変更された場合は、NIST にただちに通知するものとする。

## 5. 最終チェックリストの更新、アーカイブ、および掲載終了

NIST は、最終チェックリストの定期的な更新、アーカイブ、および掲載終了に関して以下の手順を実行する。

(a) **定期的なレビュー**：開発者は、チェックリストのステータスの変更を決定するために、少なくとも年 1 回 NIST に連絡を取る。NIST は、チェックリストのステータスの変更を決定するために、必要に応じて開発者に連絡を取ることがある。この場合、開発者は 30 日が経過するまでに返答を行い、チェックリストの更新、アーカイブ、または掲載終了を表明する。

(b) **更新**：NIST は、チェックリストが定期的なレビュー中であることを FCL に告知することがある。開発者は 60 日が経過するまでに更新された資料を NIST に提出する。更新の規模によっては、NIST がチェックリストを検査し、公開レビューのスケジュールを設定することがある。

(c) **アーカイブ**：開発者がチェックリストのサポートを提供しなくなった場合は、開発者および NIST の判断で、チェックリストをリポジトリに残しながら、アーカイブとして分類しなおすことができる。一般的な理由として、製品がサポートされなくなったり古くなったりした場合や、開発者がチェックリストのサポート提供を終了したい場合などが考えられる。

(d) **掲載終了**：NIST は、チェックリストを FCL から削除する。NIST は、NIST またはそのほかの組織によって管理されている各種のメーリングリストに告知を送信することがある。

(e) **自動的な掲載終了**：最終チェックリストに対して年 1 回のレビューが行われなかった場合、そのチェックリストは FCL から削除される。開発者および NIST の判断で、アーカイブとして分類しなおすこともできる。

## 6. 記録の保持

NIST は、プログラムに関連する情報を保持し、チェックリストプログラムの参加者にも一定の記録を保持することを要求する。詳細を以下に示す。

(a) **NIST の記録**：チェックリストが NIST に提出されている期間中、チェックリストが最終チェックリストまたはアーカイブ済みチェックリストとして FCL に掲載されている期間中、およびその後 3 年間にわたって、NIST は以下の項目を保持する。

1. リポジトリに掲載されたチェックリスト明細テンプレート
2. リポジトリに掲載されたチェックリストとチェックリスト明細
3. 公開レビュー中に提出されたすべてのコメント
4. チェックリストに関して NIST に提出されたすべてのコメント

(b) **開発者の記録**：チェックリストが NIST に提出されている期間中、およびチェックリストが最終チェックリストまたはアーカイブ済みチェックリストとして FCL に掲載されている期間中、開発者は以下の項目を保持する。

1. リポジトリに掲載されたチェックリスト明細テンプレート
2. リポジトリに掲載されたチェックリストとチェックリスト明細
3. テストレポートおよびチェックリストのテストに関するそのほかの証拠

# 付録D. 参加およびロゴ使用に関する同意書様式

この付録では、NIST チェックリストプログラムへの参加と NIST チェックリストプログラムロゴの使用に関する規約と要求事項を示す。開発者は、チェックリストを NIST に提出する前にこの付録の最新版を持っているかどうかを確認するべきである。最新版は、http://checklists.nist.gov/から独立したファイルとして入手できる。

---

National Institute of Standards and Technology

## IT 製品のための
## セキュリティ設定チェックリストプログラムへの参加
## および
## プログラムロゴの使用に関する同意書様式

バージョン 1.1
2005 年 2 月 1 日

「IT 製品のためのセキュリティ設定チェックリストプログラム」という文言および NIST チェックリストプログラムロゴは、対応するチェックリストが作成され、米国国立標準技術研究所（NIST）による IT 製品のためのセキュリティ設定チェックリスト（チェックリスト）プログラムにおけるチェックリストリポジトリへの最終的な掲載の要求事項を満たした IT 製品の特定バージョンに関連して使用されることを意図したものである。NIST チェックリストプログラムに参加し、この文言とロゴを使用するには、以下の条件に書面にて同意しなければならない。

1. NIST チェックリストプログラムの運用手順（NIST SP 800-70 の付録 C）に示したプログラムの規則および要求事項に従うこと。

2. 提出したチェックリストの公開レビューにおいて発生するコメントおよび問題に対応すること。レビュー者のコメントおよびそれに対する回答は、公開できるものとする。

3. チェックリストを管理し、チェックリストの内容に関して NIST から情報や支援を求められた場合にタイムリーに対応すること。

4. NIST チェックリストプログラムの要求事項に従って、チェックリストに関連する記録を保持すること。

5. 提出されたチェックリストに関する今後の訴訟で NIST の責任を問わないこと。

6. NIST チェックリストプログラムへの参加は、いつでも終了できる。参加終了の意志は、営業日で数えて 2 週間前までに NIST に通知すること。NIST は、提出されたチェックリストの検討または

NIST チェックリストプログラムへの参加をいつでも打ち切ることができる。NIST は、参加打ち切りの意志を営業日で数えて 2 週間前までに通知する。その場合、営業日で数えて 1 週間以内に打ち切りに対する異議申し立てと根拠となる証拠の提出を行うことができる。

7. この同意書に直接的または間接的に関連する広告、製品、またはサービスで、NIST および商務省の名前を使用してはならない。NIST は、この同意書を受け入れることにより、同意した本人、その引継ぎ人、その指定代理人、または被許諾者によって提供された、または提供される予定の製品またはサービスを直接的または間接的に推奨するものではない。この同意書がそのような製品またはサービスを推奨するものであることをいかなる方法でも暗示してはならない。NIST による推奨を暗示するような方法で本ロゴと他の標章、文言、またはロゴを組み合わせて使用してはならない。

8. 「IT 製品のためのセキュリティ設定チェックリストプログラム」という文言および NIST チェックリストプログラムロゴは、NIST の登録商標であり、NIST はこれらの独占使用権を有する。NIST は、「IT 製品のためのセキュリティ設定チェックリストプログラム」という文言および NIST チェックリストプログラムロゴの使用にかかわる品質を管理する権利を留保する。

9. NIST チェックリストプログラムへの参加の公表とロゴの使用は、対応するチェックリストが現時点で NIST チェックリストプログラムの最終チェックリストの一覧に公開されている製品および特定の製品バージョンを条件とし、それらに限って許可される。

10. NIST チェックリストプログラムへの参加の公表とロゴの使用は、チェックリスト開発者がチェックリストの適切な使用に関してチェックリストの利用者を支援すること、およびチェックリストの使用によって製品および製品の特定バージョンの保証が変更されないことを条件とし、それらに限って許可される。

11. 製品レポート、レターヘッド、パンフレット、マーケティング資料、および製品パッケージにロゴを使用する場合は、以下の文言を並記しなければならない。「TM: a Registered Mark of NIST, which does not imply product endorsement by NIST or the U.S. Government（TM：NIST の登録商標であり、NIST または米国政府による製品の推奨を意味するものではない）」

12. ロゴのサイズ、配置、色、そのほかの形状面に関する要求事項は、NIST SP 800-70 に規定されている。

13. NIST は、将来、参加費用を請求する権利を留保する。現在は無料で参加できる。過去に遡って費用を請求することはない。

14. NIST は、自らの判断で NIST チェックリストプログラムを終了できる。NIST は、プログラム条項に対する違反や法律上または規制上の理由により、参加者のプログラムへの参加を打ち切ることができる。

下記の署名により、開発者は本同意書に記載された条件に同意する。

---

組織名または会社名：

---

組織の責任者の名前および役職：

---

署名：

---

日付：

（本ページは意図的に白紙のままとする）

# 付録E. 略語および用語集

このガイドで使われている主な略語および用語を以下に定義する。一部の用語の定義は、[39]から翻案したものである。

| | |
|---|---|
| **ATP** | Advanced technology program（先端技術プログラム）、http://www.atp.nist.gov/ |
| **可用性（Availability）** | 許可されたユーザがデータや情報サービスにタイムリーかつ高い信頼性でアクセスできること |
| **候補チェックリスト（Candidate Checklist）** | NIST が公開レビューのために承認したチェックリスト |
| **CERT®/CC** | Computer Emergency Response Team/Coordination Center（コンピュータ緊急対応センター）、http://www.cert.org/ |
| **CIS** | Center for Internet Security（インターネットセキュリティセンター）、http://cisecurity.org/ |
| **CMVP** | Cryptographic Module Validation Program（暗号モジュール検証プログラム）、http://csrc.nist.gov/cryptval/ |
| **機密性（Confidentiality）** | 許可されていない個人、プロセス、または機器に対して情報が開示されないという保証 |
| **コンソーシアム（Consortia）** | IETF のような協会や団体 |
| **消費者（Consumer）** | チェックリストを使用する組織または個人 |
| **カスタム（Custom）** | 特殊化された運用環境 |
| **DHCP** | Dynamic Host Configuration Protocol（動的ホスト設定プロトコル） |
| **DHS** | Department of Homeland Security（国土安全保障省）、http://www.dhs.gov/dhspublic/ |
| **DISA** | Defense Information Systems Agency（国防情報システム局）、http://www.disa.mil/ |
| **DNS** | Domain Name System（ドメインネームシステム） |
| **FCL** | Final Checklist List（リポジトリに掲載される最終チェックリストの一覧） |
| **最終チェックリスト（Final Checklist）** | NIST がリポジトリへの掲載を承認したチェックリスト |
| **FIPS** | Federal Information Processing Standards（連邦情報処理規格）、http://csrc.nist.gov/publications/fips/ |
| **FISMA** | Federal Information Security Management Act（連邦情報セキュリティマネジメント法）、http://csrc.nist.gov/sec-cert/ |

| | |
|---|---|
| **FTP** | File Transfer Protocol（**ファイル転送プロトコル**） |
| **IDS** | Intrusion Detection System（**侵入検知システム**） |
| **IETF** | Internet Engineering Task Force、http://www.ietf.org/ |
| **独立公認レビュー者（Independent Qualified Reviewer）** | NIST によってチェックリストに関する勧告を行う任務を与えられている**レビュー者** |
| **完全性（Integrity）** | **運用中のシステムの論理的正確性と信頼性を反映するシステムまたは製品の品質、または情報の元の内容が改変または破壊されていないことの証明** |
| **内向き（Inward-Facing）** | **システムがファイアウォールの背後にあるネットワークの内部に接続されていること** |
| **LAN** | Local Area Network（**ローカルエリアネットワーク**） |
| **レガシー（Legacy）** | **通常古いシステムやアプリケーションを含む典型的なカスタム環境** |
| **ロゴ（Logo）** | NIST **チェックリストプログラムのロゴ** |
| **マネージド（Managed）** | **般に高度に構造化され、集中管理された内向きの環境** |
| **NIAP** | National Information Assurance Partnership（**全米情報保証パートナーシップ**）、http://niap.nist.gov |
| **NIST** | National Institute of Standards and Technology（**米国国立標準技術研究所**）、http://www.nist.gov/ |
| **NSA** | National Security Agency（**国家安全保障局**）、**チェックリストの入手先は** http://www.nsa.gov/snac/ |
| **NVLAP** | National Voluntary Laboratory Accreditation Program、http://ts.nist.gov/ts/htdocs/210/214/214.htm |
| **OMB** | Office of Management and Budget（**行政管理予算局**）、http://www.whitehouse.gov/omb/ |
| **運用環境（Operational Environment）** | **スタンドアロン、マネージド、またはカスタム（セキュリティを優先することによる機能制限およびレガシーを含む）** |
| **外向き（Outward-Facing）** | **システムがインターネットに直接接続されていること** |
| **PDA** | Personal Digital Assistant（**携帯情報端末**） |
| **PKI** | Public Key Infrastructure（**公開鍵基盤**） |
| **作成者（Producer）** | **チェックリストの開発者** |
| **リポジトリ（Repository）** | NIST **チェックリストリポジトリ**、http://checklists.nist.gov/ |

| | |
|---|---|
| **一般レビュー者（Public Reviewer）** | 候補チェックリストを審査し、NIST にコメントを提出する一般市民 |
| **SMTP** | Simple Mail Transfer Protocol（簡易メール転送プロトコル） |
| **セキュリティを優先することによる機能制限（Specialized Security Limited Functionality）** | 高いセキュリティニーズを受けて通常は機能が厳しく制限される特殊化されたセキュリティ要求事項を持つシステムを含む環境 |
| **スタンドアロン（Standalone）** | スモールオフィス／ホームオフィス（SOHO）環境 |
| **STIG** | Security Technical Implementation Guides（セキュリティ技術実装ガイド）、http://iase.disa.mil/stigs/index.html |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol（伝送制御プロトコル／インターネットプロトコル） |
| **テンプレート（Template）** | チェックリストの特徴を記述するための、XML 形式のチェックリスト明細テンプレート |
| **US-CERT** | DHS の CERT、http://www.us-cert.gov/ |
| **VOIP** | Voice over IP |
| **VPN** | Virtual Private Network（仮想プライベートネットワーク） |
| **WAN** | Wide Area Network（ワイドエリアネットワーク） |
| **WAP** | Wireless Access Point（ワイヤレスアクセスポイント） |
| **WEP** | Wired Equivalent Privacy |
| **WPA** | Wi-Fi Protected Access |
| **XML** | Extended Markup Language（拡張マークアップ言語） |