

Adobe Reader® および Adobe Acrobat® で PDF のセキュリティが飛躍的に向上

Acrobat X ファミリー製品の高い安全水準

目次

- 1: アプリケーションセキュリティの強化
- 4: オペレーティングシステムのアーキテクチャとの緊密な連携
- 4: 総所有コスト (TCO) の低減
- 5: 展開と管理が容易に
- 5: コンテンツセキュリティ
- 6: まとめ

Adobe Reader X および Adobe Acrobat X の新たなセキュリティ機能は、PDF ベースのマルウェアがもたらす危険性を軽減します。

Adobe Reader X および Adobe Acrobat X では、PDF ドキュメントおよびデータのセキュリティが飛躍的に向上しています。Adobe Reader X および Adobe Acrobat X はセキュリティを重視する体制のもとで開発されており、最先端の「サンドボックス」技術と、きめ細かい制御能力、Microsoft® Windows® および Mac OS X の両アーキテクチャとの緊密な連携、パッチ適用の効率化、展開および管理ツールの改良によって、強力なアプリケーションセキュリティが実現されています。Adobe Reader X および Adobe Acrobat X の新機能を利用すると、従来バージョンの Adobe Reader X および Adobe Acrobat X 製品と比較して総所有コスト (TCO) を低減できます。

さらに、アドビ製品使用時のデータの安全性を確保するために、Adobe Secure Software Engineering Team (ASSET) および Adobe Product Security Incident Response Team (PSIRT) の両チームが協力して取り組んでいます。アドビでは、自社でセキュリティへの取り組みを進めるのに加えて Microsoft Active Protections Program (MAPP) にも協力し、ウイルス対策ベンダー、侵入検知・防止策ベンダーなどセキュリティソフトウェアプロバイダーとの間で製品の脆弱性に関する効果的な情報共有を行っています。これにより、業界を挙げての協力のもとで Adobe Acrobat X および Adobe Reader X の脆弱性リスクを低減していく体制が確立しています。

アプリケーションセキュリティの強化

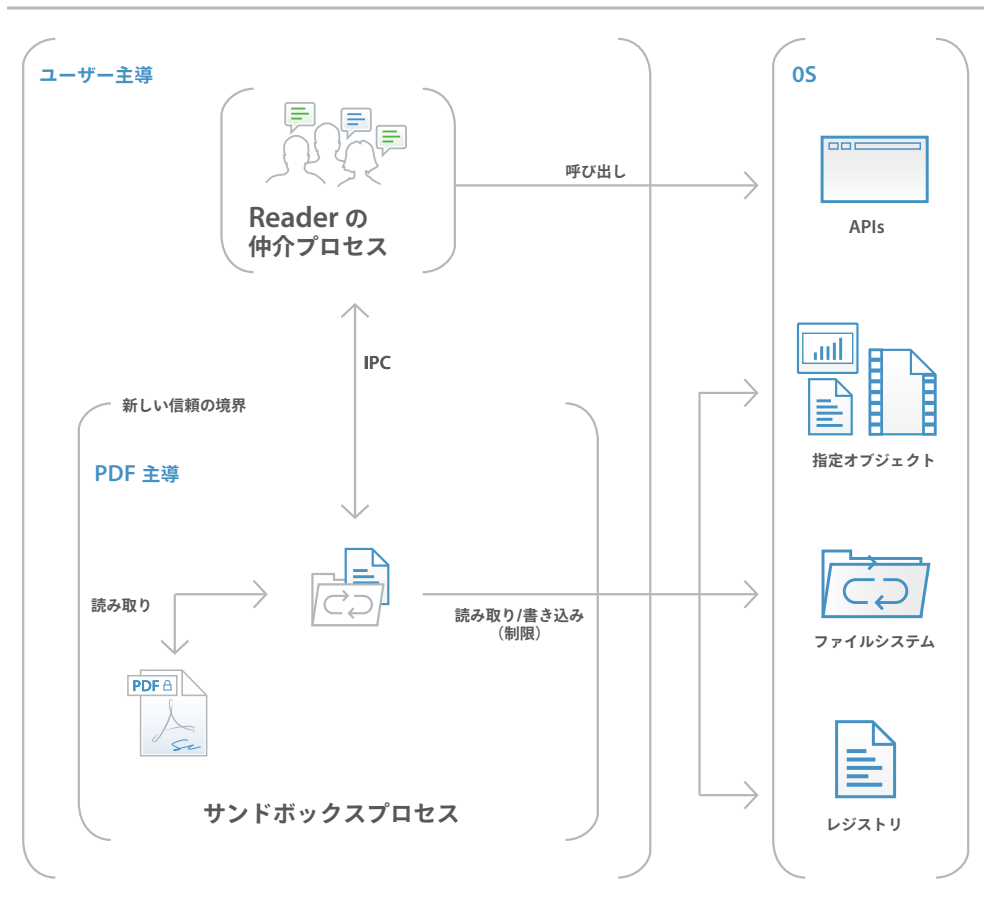
Adobe Reader X の保護モード

悪意のあるコードには、PDF ファイルを利用してコンピューターのファイルシステムへの書き込みを試みるものがあります。このようなコードからユーザーおよびユーザーが属する組織を保護するために、アドビでは、保護モードと呼ばれる一種の「サンドボックス」技術を製品に実装しています。

Adobe Reader X の起動時、保護モードは初期設定で有効になっています。このモードを利用すると、攻撃者はユーザーのシステムにマルウェアをインストールすることができなくなり、潜在的なセキュリティ脅威の危険性が軽減します。特に、保護モードでは、プログラムに付与されるアクセスレベルを制限することで、コンピューターのファイルシステムへの書き込み、ファイルの削除、システム情報の改ざんなどを試みる悪意のある PDF ファイルから、Microsoft Windows オペレーティングシステムで動作するシステムを保護します。

サンドボックスとは

サンドボックスとは、隔離した環境の中で権限またはセキュリティ特権を低下させた状態でプログラムを実行する手法の1つであり、セキュリティ専門家間で高く評価されています。サンドボックスを使用すると、実行可能コードを含んだ信頼のおけないドキュメントによってユーザーのシステムが侵害されるのを防ぐことができます。Adobe Readerの場合、信頼されないコンテンツとは、あらゆるPDFファイルとそこから起動されるプロセスを意味します。Adobe Reader Xでは、すべてのPDFを潜在的に有害であると見なし、PDFの処理をすべてサンドボックス内で実行します。



またアドビでは、製品ライフサイクルのあらゆる段階にセキュリティ機能を組み込む、Adobe Secure Product Lifecycle (SPLC) プロセスに取り組んでおり、その一環として、既存コードの定期的な再評価と必要に応じた強化を行っています。これにより、アドビ製品使用時のアプリケーションセキュリティがさらに強化され、データの安全性も向上します。

Adobe Acrobat Xの保護されたビュー

保護されたビューとは、Adobe Readerの保護モードと同じくサンドボックス技術の実装の一種です。保護されたビュー機能はAcrobat Xバージョン10.1に実装されており、Adobe Acrobatの豊富な機能に対応しています。保護されたビューでも、保護モードと同じく、信頼のおけないプログラム（例えば、あらゆるPDFファイルとそこから起動されるプロセス）を、機能制限されたサンドボックスの中に隔離して実行します。この仕組みが、PDF形式を利用した悪意あるコードによってコンピューターのファイルシステムへの書き込みが実行されるのを防ぎます。

保護されたビューは、悪意あるコードがどのPDFファイルにも含まれる潜在的な可能性があることを前提に機能するので、具体的な個別のファイルに対するユーザーが信頼性を判断した場合以外はサンドボックス内で処理を実行します。保護されたビューは、単体のAdobe Acrobat Xアプリケーション上でユーザーがPDFドキュメントを開く場合と、ブラウザ上で開く場合の両方をサポートしています。ユーザーから見た使い勝手には、それぞれの場合で若干の違いが生じます。

単体のAdobe Acrobat Xアプリケーションでは、悪意を含んでいる可能性があるファイルを保護されたビューで開くと、表示ウィンドウの上部に黄色いメッセージバー（YMB）が表示されます。このバーは、それが信頼のおけないファイルであることと、現在は保護されたビューで動作しているのでAcrobatの機能の多くが無効化され、ファイルに対する操作が制限されることを示しています。簡単にいえば、ファイルは読み取り専用モードで表示され、悪意ある埋め込みコンテンツや付随するコンテンツがシステムに手を加えることはできないようになります。ファイルを信頼してAdobe Acrobat Xの機能をすべて有効にするには、YMB上の「すべての機能を有効にする」ボタンをクリックします。すると、保護されたビューが終了し、Acrobatでセキュリティ特権付きとして扱われる場所のリストにそのファイルが追加されて、ファイルに対する永続的な信頼が設定されます。以後、信頼されたPDFを開くときには、保護されたビューによる制限が適用されません。

PDFファイルをブラウザで開く場合、保護されたビューは、YMBを必要としないスムーズな方法で動作します。このときブラウザ環境の上では、すべてのAdobe Reader機能と、ドキュメントの作成者がAcrobat上でReaderユーザーに許可した拡張機能（既存フォームフィールドへの署名、署名フィールドの新規追加、フォームデータの保存など）を利用できます。

アドビの

JavaScript 制御機能

アドビの JavaScript 制御機能では、次の操作を行うこともできます。

- ・ JavaScript エンジンのオン/オフを切り替える
- ・ JavaScript から起動される URL の有効/無効を切り替える
- ・ セキュリティ特権の高い JavaScript の実行を、他のアクセス許可とは別個に制御する
- ・ 証明済みドキュメントの上ではセキュリティ特権の高い JavaScript を有効にする

柔軟な設定機能により、信頼できるファイル、フォルダー、ホストなどの場所に対しては、これらの制限の適用を選択的に除外することができます。

JavaScript の実行

Adobe Acrobat X ファミリーでは、Windows 環境でも、Mac OS X 環境でも、JavaScript の実行をきめ細かく制御できます。Adobe JavaScript ブラックリストフレームワークは、ビジネスワークフローの中で JavaScript を使用できるようにしつつ、特定の JavaScript API 呼び出しを狙った攻撃からユーザーとシステムを保護する仕組みです。

特定の JavaScript API 呼び出しをブラックリストに追加すれば、その呼び出しの実行はブロックされます。JavaScript を完全に無効にする必要はありません。特定の JavaScript API 呼び出しをブロックする設定を個々のユーザーが上書きできないようにして、組織全体を悪意のあるコードから保護することもできます。ブラックリストは、Windows 環境では Windows レジストリで管理され、Mac OS X 環境では、Mac OS X FeatureLockdown ファイルに保存されます。

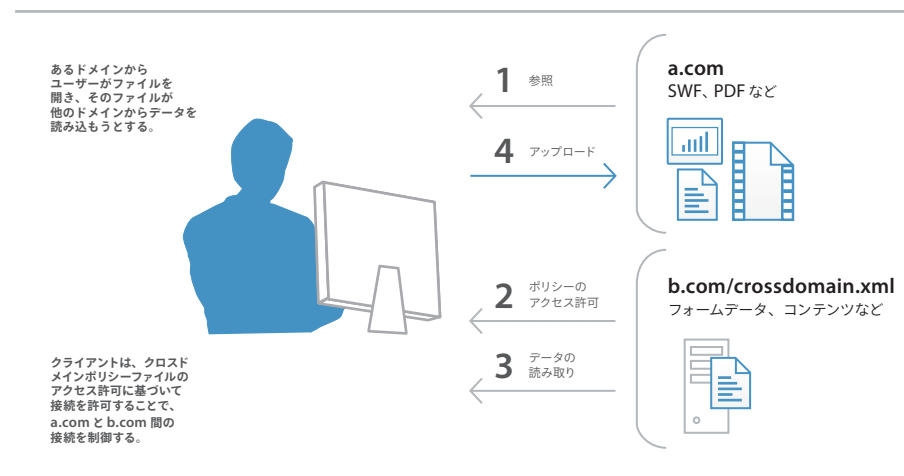
クロスドメイン構成

Adobe Acrobat X ファミリー製品では、Microsoft Windows クライアントでも Mac OS X クライアントでも、無制限のクロスドメインアクセスは初期設定で無効になっています。これは、攻撃者が PDF ファイルを利用して他のドメインのリソースにアクセスすることを防止するためです。

Adobe Acrobat X および Adobe Reader X には、サーバーベースのクロスドメインポリシーファイルをサポートする機能が組み込まれており、ドメインをまたいだデータ処理が必要な場合はポリシーファイルによって許可できます。クロスドメインポリシーファイルは、リモートドメインに置かれる XML ドキュメントです。これを使用すると、ソースドメインにアクセスし、Adobe Acrobat X または Adobe Reader X のトランザクションを続行することが可能になります。

次のような場合には、アドビのクロスドメインサポートを有効にする必要があります。

- ・ 特定のドメイン間でクロスドメインアクセスを行うことや、デジタル証明書に基づく認証などの機能を利用することが必要な場合
- ・ クロスドメインのアクセス許可をサーバーベースの単一の場所で一元管理する必要がある場合
- ・ フォームデータの返信を求める複数のドメインからのデータリクエスト、SOAP リクエスト、ストリーミングメディアの参照、Net.HTTP リクエストなどのワークフローを実装する場合



わかりやすいセキュリティ警告

Adobe Acrobat X ファミリー製品では、操作を妨げない黄色いメッセージバー（YMB）に、セキュリティの警告がわかりやすく表示されます。従来のダイアログボックスと異なり、この YMB はページのコンテンツを遮ることがないため、警告をすばやく確認して対応できます。

Adobe Acrobat X および Adobe Reader X クライアントでは、ドキュメントの上部に、警告またはエラーメッセージの YMB が表示されます。ユーザーは、このドキュメントを 1 回だけ信頼するか、常に信頼するかを選択できます。常に信頼することを選択した場合、ドキュメントは、セキュリティ特権扱いのドキュメントとしてリストに追加されます。

拡張セキュリティが有効になっている場合、セキュリティ特権扱いになっていない（例：信頼済みでない）PDF が次のような処理を実行しようとする、潜在的な危険性があることを示す YMB が表示されます。

- ・ クロスドメインアクセスの開始
- ・ JavaScript の実行
- ・ JavaScript によって呼び出された URL の呼び出し
- ・ ブラックリストに含まれる JavaScript API の呼び出し
- ・ データのインジェクション
- ・ スクリプトのインジェクション
- ・ 従来形式の埋め込みマルチメディアの再生

ユーザーは、このドキュメントを 1 回だけ信頼するか、常に信頼するかを「オプション」ボタンで選択できます。また、企業全体でファイル、フォルダー、ホストに関する信頼を事前設定すれば、信頼済みの企業ワークフローにおいて YMB が表示されるのを防ぐことができます。

オペレーティングシステムのアーキテクチャとの緊密な連携

常時作動のセキュリティ

Adobe Acrobat X ファミリー製品には、デスクトップシステムの制御やメモリの破壊を試みる攻撃に対して追加の防御レイヤーが備えられており、Microsoft Windows でも Mac OS X でも、組み込みの常時作動セキュリティ保護機能を利用できます。

- ・ データ実行防止（DEP）は、Windows オペレーティングシステムで「保護」扱いとされているメモリ領域にデータや危険なコードが配置されるのを防ぐ機能です。Apple Mac OS X 10.6 でも、64 ビット版 Safari ブラウザーには同様の実行可能ファイル保護機能が備わっています。
- ・ Address Space Layout Randomization（ASLR）は、システムコンポーネントのメモリやページファイルがある場所を攻撃者に発見されにくくする機能です。ASLR は Windows と Mac OS X 10.6 の両方に採用されています。

レジストリレベルの構成と plist 構成

Adobe Acrobat X ファミリー製品には、レジストリレベル（Windows）および plist（Macintosh）によるセキュリティ設定を管理するための様々なツールが用意されています。これらの設定方法を使用すると、展開の前後に次のようなクライアントの設定を行うことができます。

- ・ 拡張セキュリティを有効または無効に切り替える
- ・ セキュリティ特権扱いの場所を有効または無効に切り替える
- ・ 事前定義されたセキュリティ特権扱いの場所を指定する
- ・ 特定の機能をロックしてアプリケーション UI を無効化し、エンドユーザーによる設定変更ができないようにする
- ・ その他ほぼすべてのセキュリティ関連機能について、有効と無効の切り替えや他の設定操作を行う

総所有コスト（TCO）の低減

ソフトウェアセキュリティの堅牢化

Adobe Reader の保護モードや Acrobat の保護されたビューのようなセキュリティ機能強化は、今後の脅威に対して Acrobat 製品ファミリーの堅牢性を高めるためにアドビが行っている様々な取り組みのごく一部に過ぎません。ソフトウェアが攻撃に強くなれば、システムの運用停止を伴うセキュリティ更新の必要性を低減または排除することができ、定期的な更新についても緊急度を下げることができます。そうした対策全般が運用の柔軟性向上と TCO の低減につながり、特に、セキュリティ保証の要件が厳しい大規模な運用環境では非常に大きな効果があります。

Microsoft SCCM および SCUP のサポート

Adobe Acrobat X ファミリー製品では、Microsoft System Center Configuration Manager（SCCM）を使用して効率よく更新プログラムを読み込み、配布することができます。これにより、管理対象の Windows デスクトップに常に最新のセキュリティパッチや更新プログラムを適用した状態を保つことができます。

Microsoft System Center Updates Publisher (SCUP) カタログを新たにサポートしたことで、組織全体に展開した Adobe Acrobat X および Adobe Reader X の更新を自動化でき、導入当初の展開作業も効率的に実行できます。SCUP はアドビから発行される更新プログラムを即座に自動的に読み込めるので、導入した Adobe Acrobat X および Adobe Reader X の更新作業を簡単に、効率よく行うことができます。新たに提供された SCCM および SCUP との統合機能を活用すれば、組織全体に対して簡単、迅速にパッチを適用できるので、アドビソフトウェアの TCO 低減効果を期待できます。

Apple Package Installer および Apple Remote Desktop のサポート

Adobe Acrobat X ファミリー製品では、独自の Adobe Installer に代わって、Mac OS X に標準装備されている Apple Package Installer が採用されました。これにより、Adobe Acrobat および Adobe Reader を企業内の Macintosh デスクトップに導入する作業が容易になります。最初のソフトウェア導入も、その後のアップグレードおよびパッチ適用も、Apple Remote Desktop 管理ソフトウェアを使用して一元的に実行できます。

導入と管理が容易に

定期的に行われる累積ソフトウェア更新およびパッチ

ソフトウェアが最新の状態に維持されるよう、アドビでは、機能のアップグレードやセキュリティの修正を含む更新プログラムを定期的に配信しています。また、ゼロデイ攻撃に早急に対応するために、必要に応じてパッチも提供しています。システムを最新の状態に保つための手間とコストを抑えられるように、提供するパッチにはできるだけ累積的な内容を含めています。セキュリティパッチが既存のインストール環境やワークフローになるべく影響しないように、リリース前のパッチに対しては厳しいテストを実施しています。

また、次の Web サイトおよび通知サービスも利用できます。

アドビ製品の最新のセキュリティ情報については、www.adobe.com/jp/support/security/ をご覧ください。

セキュリティに関する最新のレポートや脆弱性の修正については、Adobe PSIRT ブログ (blogs.adobe.com/psirt/) (英語) をご覧ください。

アドビ製品とセキュリティ機能について詳しくは、アドビセキュリティライブラリ (www.adobe.com/go/learn_acr_appsecurity_jp) (英語) をご覧ください。

Adobe Customization Wizard および AIM (英語版でのご提供)

アドビでは、企業における大規模運用をいっそう的確に管理するために役立つ次のツールを提供しています。

- Adobe Customization Wizard—無料でダウンロードできるユーティリティです。Acrobat のインストーラーをカスタマイズして、導入前にアプリケーションの機能を構成できます。
- Administrator's Information Manager (AIM) —カスタマイズ可能な自動更新型の Adobe AIR® アプリケーションです。環境設定リファレンスが収録されています。また、大企業の管理者に役立つ様々なリソースが付属し、その内容は随時拡充されています。

コンテンツセキュリティ

アプリケーションセキュリティに加え、アドビでは、電子署名、権限の管理、およびドキュメントのベストプラクティスなど、PDF ドキュメントに含まれる情報の保護や認証に役立つ業界標準のメカニズムも多数サポートしています。

電子署名

電子署名を活用すると、手書きの署名よりも時間や費用を節約でき、改ざんのない正当なドキュメントコンテンツが受領されたことをドキュメントの作成者と受領者の双方が確認できます。Adobe Reader X および Adobe Acrobat X では、電子署名をドキュメントに追加して、署名の有効性を確認し、許可や制限を追加することで、署名ワークフローを簡単に制御することができます。

権限の管理

Adobe Acrobat X ファミリー製品では、Adobe LiveCycle® Rights Management ES2 サーバーソフトウェアの権限管理機能を利用して機密データを保護し、外部への漏洩や悪用を防ぐことができます。データに対するアクセス、印刷、コピーおよび編集操作の可否を、ドキュメント単位、ユーザー単位、グループ単位のいずれかで管理でき、使用されているドキュメントについても管理ポリシーを動的に変更できます。しかも、Adobe Reader があればコンテンツには誰でも安全にアクセスできます。保護されたドキュメントを参照するのは簡単で、受信者が追加の製品やプラグインを購入したりダウンロードしたりする必要はありません。

一貫したベストプラクティス

Adobe Acrobat X の新たなアクションウィザード機能を使用すれば、ドキュメントのプロセスを簡単にスクリプト化して、組織全体に展開できます。これにより、一般公開用のドキュメントはベストプラクティスに従って作成および保護されることになります。

機密情報の管理

削除ツールや強力な墨消しツールを使用して、ファイル内の機密情報を一貫してすばやく削除できます。強力な標準ベースの暗号化技術により、エンドユーザーは、パスワードとアクセス許可を設定して PDF ドキュメントへのアクセスを制御したり、変更を禁止できます。

まとめ

Adobe Acrobat X ファミリー製品では、PDFドキュメントおよびデータのセキュリティが飛躍的に向上しています。強力なアプリケーションセキュリティ、きめ細かい制御、オペレーティングシステムとの緊密な連携など、Adobe Acrobat X および Adobe Reader X には、セキュリティを重視する体制のもとで開発された様々な機能が盛り込まれています。Adobe Reader X および Adobe Acrobat X では、アプリケーションセキュリティの向上、OS 連携機能の強化、バッチ適用の効率化、展開および管理ツールの改良により、従来の Adobe Reader および Adobe Acrobat 製品と比較して総所有コスト (TCO) を大幅に低減できます。

また、Adobe Acrobat X および Adobe Reader X の開発は、アドビが擁する製品セキュリティ専門家集団である Adobe Secure Software Engineering Team (ASSET) の支援のもとで行われています。ASSET は、Adobe Product Security Incident Response Team (PSIRT) とも協力しながら、ユーザーデータの安全性とセキュリティをあらゆる場面で確保できるようにするための活動を展開しています。



詳細情報

ソリューションの詳細：www.adobe.com/jp/security

アドビ システムズ 株式会社
〒141-0032 東京都品川区大崎 1-11-2
ゲートシティ大崎イーストタワー
www.adobe.com/jp
Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Adobe, the Adobe logo, Acrobat, Adobe AIR, AIR, LiveCycle, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Apple, Mac OS, and Macintosh are trademarks of Apple Inc., registered in the U.S. and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2011 Adobe Systems Incorporated. All rights reserved. Printed in Japan.