Appleテクニカルホワイトペーパー

OS Xのセキュリティ

2012年3月8日（火）

目次

OS Xのセキュリティの概要 3

安全なデータストレージ 4

- FileVault 2 4
- コンテナの暗号化—ディスクイメージ 5
- 確実にゴミ箱を空にする 6
- 確実な消去 6
- リモートロックおよびリモートワイプ 7
- アプリケーション制限 7

公開鍵インフラストラクチャ 8

- デジタルID. 8

キーチェーン 9

コード署名およびアプリケーション署名 10

ファイアウォール 11

- アプリケーションレイヤーのファイアウォール 11
- IPFW2ファイアウォール 12

コアセキュリティ 12

- 強制アクセス制御 13
- サンドボックス 13
- 実行の無効化 14
- ライブラリのランダム化 14
- アドレス空間レイアウトのランダム化 15

マルウェア防止 15

- アプリケーションの隔離 15
- マルウェアの識別と削除 15
- ウイルス対策保護 16

プライバシー 16

- 位置情報サービス 16
- オンラインプライバシー 16

結論 17

OS Xのセキュリティ

AppleはOS Xの設計にあたり、最初からシステムセキュリティの装備と維持に配慮しました。このアプローチでは、オペレーティングシステムの各レイヤーにセキュリティ機能を設計段階で組み込み、可能な限りセキュリティを簡単に自動的に利用できるようにすることを基本思想としています。Appleはこの「後付けではなく、統合されたセキュリティ機能」というアプローチを念頭に置き、ユーザによる高度な設定や複雑な操作なしに、オペレーティングシステムのコアが、サービス、アプリケーション、データに対して重要な保護を確実に提供するように努力しています。

このホワイトペーパーでは、安全なデータストレージ、公開鍵インフラストラクチャ（PKI）、ファイアウォール、強制アクセス制御によって強化されたコアのマルウェア防御テクノロジーなど、OS Xに実装された様々なセキュリティテクノロジーについて説明します。これらのセキュリティテクノロジーは、階層型のセキュリティモデルに構築することができます。組織のセキュリティ戦略の検討にあたっては、利用できるすべてのセキュリティ上の選択肢を調査し、セキュリティに関する組織のニーズと、予測される管理オーバーヘッドやユーザに対する影響とのバランスを取る必要があります。

OS Xのセキュリティの概要

OS Xでは、外部のセキュリティ上の脅威に対して、一連の保護システムが実効性のある防御策を実行します。このような防御策には、認証とアクセス制御のシステム、ネットワーク経由の脅威を制限するための機能のほか、システムライブラリのランダム化、アドレス空間レイアウトのランダム化（ASLR）、サンドボックス、マルウェアの可能性があるファイルの隔離などのランタイムメカニズムがあります。Appleのエンジニアは、多様なアプローチを駆使して潜在的なセキュリティ上の脅威を特定し、それらの脅威から積極的にOS Xコンポーネントを保護します。

OS Xおよびその統合サービスの多くは、FreeBSD、Apache、Kerberosなどのオープンソースソリューションの基盤の上に構築されています。この基盤は、数年にわたって世界中の開発者やセキュリティ専門家の厳しい目にさらされ、セキュリティが強化されてきました。強力なセキュリティは、オープンソースのソフトウェアが持つメリットの1つです。オープンソースのソフトウェアは、セキュリティの専門家や開発者が自由にソースコードを調べて理論的な脆弱性を特定し、ソフトウェアを強化する措置が取れるからです。Appleはこのオープンソースコミュニティに積極的に参加し、OS Xのアップデートを定期的にリリースして社外の開発者の継続的なレビューに提供するとともに、改善意見を取り入れています。オープンソースによる開発アプローチでは、OS Xが可能な限りの安全性を装備するために必要な透明性が確保されます。Appleは一般に誤解されているような、「不知によるセキュリティ」の理念は採用していません。

従来の閉鎖的な、単一ベンダーによるデスクトップオペレーティングシステムのレビューモデルでは、脆弱性を悪用した攻撃がたびたび報告されていますが、このオープンアプローチはそれとはまったく対照的です。OS Xのユーザは、ソースベンダーのみが行う非公開のテストに依存するのではなく、数多くのセキュリティの専門家や

バージョン別セキュリティガイド

Appleでは、OS Xのバージョン別のセキュリティ構成ガイドを提供しています。これらのガイドでは、Macシステムのセキュリティ設定を強化する様々な方法を網羅し、より詳しく説明しています。これらのガイドは、www.apple.com/support/security/guides/ で入手できます（英語）。各セキュリティガイドは、Appleと米国国家安全保障局（NSA）の共同作業による検討と検証の結果です。これらのガイドは、NSAの情報保証Webサイト（http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml）でも提供されています。

セキュリティ組織による継続的で公開された検証の成果を利用することができます。その結果、生来的に安全性の高いオペレーティングシステムが誕生します。

またAppleは、コンピュータ緊急対応チーム／調整センター（CERT/CC）、コンピュータセキュリティインシデント対応チーム協議会（FIRST）、FreeBSDセキュリティチーム、さらには、米国国土安全保障省や国家安全保障局などの、米国連邦政府のセキュリティの専門家をはじめとする多くのセキュリティ組織と協力しています。

OS Xは、データがローカルボリュームに保存されている間（「静的に保存されているデータ」）はもちろん、インターネットでの伝送中も（「送信中のデータ」）、USBハードドライブやフラッシュハードドライブに保存して移動するときも、ローカルネットワークでの共有時にも、ユーザとそのデータの機密を保護するための複数の機能を搭載しています。これらのテクノロジーは、オペレーティングシステムで常に有効なものもあれば、オプションとして提供され、Macに保存されているデータまたはMacからアクセスするデータのセキュリティの強化に使用されるものもあります。1つの主要な例が、ローカルディスクを暗号化する「FileVault」です。

安全なデータストレージ

OS X Lionには、Macシステムに保存されているファイルをAES（Advanced Encryption Standard）を使用して安全に保護する使いやすい機能が搭載されています。この機能はユーザにほとんど意識されることなく動作します。また静的に保存されているデータを暗号化するだけでなく、コンピュータを組織内で別の用途に転用する場合や、コンピュータを売却や譲渡などによって処分する場合に、すべてのデータを復元できないように確実に消去するオプションも提供されています。

「FileVault 2」

OS X Lionで導入された「FileVault 2」は、静的に保存されているデータ（DAR）をボリューム全体の暗号化によって保護する機能です「FileVault 2」では、Macシステムの紛失、盗難の際にも、すべてのデータを保護できるように、XTS-AES-128データ暗号化がディスクレベルで採用されています （「FileVault 2」は、外部USBドライブおよびFireWireドライブでもサポートされています）。

システムに機密データが保存される場合は、「FileVault 2」を採用し、使用を義務付けることを検討してください。

「FileVault 2」による最初の暗号化は、ユーザに意識されることなく高速に処理されます。すべてのデータは、バックグラウンドで暗号化されます。「FileVault 2」は、バランスのとれたシステム性能を実現するため、ファイルのコピーや参照などの優先順位の高いユーザタスクを優先し、プロセッササイクルを放棄します。ボリュームの最初の暗号化が完了すると、それ以降作成されるファイルはすべて自動的に暗号化されます。

「FileVault」の初期設定の際、ユーザがパスワードを忘れた場合や使用できない場合に備え、暗号化されたボリュームにアクセスするための復旧キーが統合されます。復旧キーのアプローチには、個人用

の復旧キーを使った個人向けのアプローチと、団体の復旧キーを使った団体向けのアプローチの2種類があります。

個人向けの復旧方法を選択すると、ユーザがログイン用の認証情報を忘れたときに使用する復旧キーが自動的に生成されます。この復旧キーは、ユーザが手動でコピーして保存できます。あるいは、Appleのサーバに送信して保護された状態で保存し、必要なときに権限を持つユーザが取得することもできます。

「FileVault 2」を有効にした場合、コンピュータでファイルにアクセスし、起動プロセスを続行するには、ユーザが有効なログイン認証情報または復旧キーを入力する必要があります。ログイン認証情報または復旧キーを入力しない限り、暗号化されたデータは一切復旧できません。ボリューム全体が暗号化され、不正なアクセスから保護された状態が維持されます。

「FileVault 2」はまた、IT部門がいつでも特定のMacから暗号化キーを消去できる機能を提供します。この場合、暗号化されたデータは、ユーザログインによっても、データ復旧ツールによってもアクセスできなくなります。このプロセスは、リモートワイプと呼ばれます。

「FileVault 2」で保護されたシステムでは、バックアップユーティリティの最初の起動前認証の待機中にアクセス不能になり、自動バックアップソリューションが機能しなくなることがあります。そのような場合、ユーザがログインしている間のみバックアップが実行されるように、バックアップ方法を変更する必要があります。

コンテナの暗号化—ディスクイメージ

「ディスクユーティリティ」ツールを使用すると、128ビットや、さらに強力な256ビットのAES暗号化を使用して、「ディスクイメージ」と呼ばれる暗号化されたコンテナを簡単に作成できます。ディスクイメージはシステム上のローカルボリュームとしてアクセスし、コピーや移動を実行したり、開いたりすることができます。

基盤となるディスクイメージを暗号化すると、そのディスクイメージに保存したファイルやフォルダの暗号化と復号化が自動実行されます。ディスクイメージの内容（ファイル名や日付、サイズ、その他のプロパティなど）を表示するには、ロック解除用のパスワードを入力するか、あらかじめキーチェーンの中に対応する暗号化キーを設定しておく必要があります （詳しくは、このホワイトペーパーの「キーチェーン」のセクションを参照してください）。

ディスクイメージを復号化した場合、必要に応じてファイルデータがブロック単位でリアルタイムに復号化されます。たとえば、暗号化されたディスクイメージからQuickTimeムービーを開いた場合、そのムービーファイルの現在再生中の部分のみが復号化されます。データは常に静的に暗号化され、ファイルシステムから露出することは絶対にありません。

この暗号化と復号化のプロセスは、ユーザの介入なしに自動的に実行されます。ユーザの操作が必要なのは、ロック解除用のパスワードまたは暗号化キーが保存されたキーチェーンのロック解除用認証情報を求められた場合のみです。この機能を使って暗号化したディスクイメージをリムーバブルメディアに入れて持ち運んだり、Mac上

やネットワークファイルサーバに保存したりすることで、ドキュメント、ファイル、フォルダを安全に交換できます。

暗号化されたディスクイメージの作成は簡単です。「ディスクユーティリティ」で「新規イメージ」をクリックし、作成するディスクイメージのサイズとタイプを選択し、ポップアップメニューから暗号化オプション（「128ビット」、「256ビット」、「なし」のいずれか）を選択します。ここで、作成するイメージのパスワードを入力するように求められます。「ディスクユーティリティ」の中でOS Xのパスワードアシスタントを使えば、暗号化されたディスクイメージ用の強力なパスワードを作成できます。

また暗号化されたディスクイメージをさらに詳細に管理する場合は、コマンドラインのhdiutilツール（OS X「ターミナル」ユーティリティまたはリモートSSHセッションを使用）によって、基盤となるディスクイメージフレームワークにアクセスできます。「`man hdiutil`」と入力すると、hdiutilのマニュアルページが表示され、ポリシーに準拠する暗号化されたイメージの自動化と作成に使用できるすべてのオプションのリストを参照できます。

暗号化されたバックアップ—「Time Machine」

OS Xに内蔵のバックアップユーティリティ、「Time Machine」を使用すると、Macシステムからローカルのハードドライブやネットワークドライブへのバックアップが自動的に実行されます。「Time Machine」へのバックアップの方法は、OS Xでクライアント管理ソリューションを使って手動または自動で設定できます。バックアップの暗号化は、「FileVault 2」の機能の1つです。OS X Lionでは、特別なハードウェアを使用しなくても、既存のストレージメディアで「Time Machine」のバックアップ全体を暗号化できます。バックアップの暗号化を使用すると、「FileVault 2」はバックアップディスク全体を暗号化します。

確実にゴミ箱を空にする

OS Xの「確実にゴミ箱を空にする」コマンドは、削除したファイルを復元できないように処理します。通常、コンピュータからファイルを削除すると、ファイル名と保存場所はディスクのディレクトリから削除されますが、ファイル自体は、それが存在するハードディスク上の場所に別のファイルが保存されるまで、そのままの状態で放置されます。誤ってファイルを削除した場合、市販のユーティリティを使って、これらの「削除」したはずのファイルを検索して復旧することができます。しかしそれは同時に、権限のないユーザが削除したファイルを復旧できることを意味し、セキュリティ上のリスクとなります。

「確実にゴミ箱を空にする」コマンドは、磁気メディアのサニタイズに関する米国国防総省の規格に準拠し、削除するファイルが入ったブロックに7回にわたって繰り返し書き込みを行います。

これと同じ機能や、ファイルやディレクトリを確実に消去するさらに高度な管理機能をコマンドラインから利用できます。「`man srm`」と入力すると、srm（安全な削除を意味する「secure remove」の略）のマニュアルページが表示され、ファイルの安全な上書きに使用できるすべてのオプションのリストを参照できます。

確実な消去

コンピュータからファイルを削除しても本当に削除されないのと同様、ハードドライブを消去しても、それに保存されているデータが本当に削除されるわけではありません。実際のところ、ドライブからデータを消去することはできません。できるのは、新しいデータを古いデータの上にコピーすることだけです。したがって、ドライブまたはボリュームを完全に「消去」する必要がある場合、古いデータの上に意味のない新しいデータをコピーするプロセスを使用する必要があります。

「ディスクユーティリティ」には古いデータを確実に消去する様々なオプションが用意されていて、ドライブやボリューム全体を対象とすることも、（削除済みのデータがあった領域を含め）未使用領域のみを対象とすることもできます。

「ディスクユーティリティ」の「確実な消去」の機能には、次のオプションがあります。

- **最も速い。**ドライブやボリュームを消去または再フォーマットする場合に実行されるデフォルトの処理です。この方法ではディスク復旧アプリケーションが持つセキュリティ機能は使用されず、ドライブやボリュームがほとんど即座に消去されます。
- **データをゼロ消去。**このオプションでは、すべてのデータに対して0（ゼロ）を1回書き込みます。「確実な消去」のオプションのうち処理は最速ですが、提供されるセキュリティのレベルは最小限に留まります。
- **3回消去。**このオプションでは、DOE準拠の3回の「確実な消去」を実行します。ディスク全体または空き領域に、最初の2回はランダムデータを、最後の1回は既知のデータを書き込みます。
- **最も安全。**このオプションでは、0、1、ランダム情報のうち事前に設定した文字を7回にわたってドライブに書き込みます。このオプションは、磁気メディアの確実な消去に関する米国国防総省の規格（DOD 5220-22M）に適合しています。このプロセスでは複数回の書き込みが行われるので、時間がかかることがあり、「データをゼロ消去」のオプションの7倍の時間がかかります。

リモートロックおよびリモートワイプ

OS X Serverを使用する場合、組織のIT部門は、システムの紛失または盗難の際に、ユーザがウェブサイトからシステムをリモートにロックし、さらにはワイプできるように設定できます。

IT部門がユーザのMacに対してこのオプションを設定すると、ユーザはセルフサービスウェブサイトにアクセスして、システムのロックやワイプを実行できるようになります。この方法では、ユーザは使用する機器に問題が発生したときに、IT部門によるアクションを待たずに、即座に対応することができます。

一方IT部門は、ユーザの介入なしに、プロファイルマネージャを使用して離れた場所にあるMacのロック、ロック解除、ワイプを実行できます。またコマンドを実行したのがユーザか管理者かに関係なく、ロックやワイプのコマンドの状態をモニタできます。

アプリケーション制限

IT部門は、アプリケーションの場所や署名など、多様な要素に基づいて、ユーザが特定のアプリケーションを起動できないように阻止できます。このような制御により、管理者はユーザがアプリケーションをインストールした方法や場所に関係なく、未承認のアプリケーションの実行を防止できます。この機能は一般に、ホワイトリスト方式によるアプリケーション制限と呼ばれます。IT部門はこの機能をプロファイルを使って制御する他のポリシーと組み合わせて使用することで、ユーザのMacで実行できるアプリケーションをきめ細かく管理できます。

公開鍵インフラストラクチャ

公開鍵インフラストラクチャ（PKI）とは、デジタル世界における物理エンティティの識別情報と現在の信頼関係を確認するための、すべてのコンポーネント（ハードウェア、ソフトウェア、ポリシー、プロセス）およびそれらのコンポーネント間で実行される複雑な相互関係です。

デジタルID

PKIの基盤は、「デジタルID」です。これはデジタル証明書とそれに対応する公開鍵および秘密鍵で構成されます。

OS XにおけるPKI

OS XはオペレーティングシステムベースのPKIです。つまり証明書とアイデンティティを解析、解釈、検証、信頼するためのすべてのサービスが、個別のアプリケーションではなく、オペレーティングシステムによって実行されます。このアプローチでは、X.509ベースのアイデンティティによるセキュリティが強化されるとともに、すべてのアプリケーションにわたって単一のシームレスなサービスが提供されます。OS Xには、ECC（Elliptical Curve Cryptography）などの、新しい安全性の高い暗号化標準が導入されたので、アプリケーション開発者による独自のソリューション構築を待つことなく、システム全体でその新しい暗号化標準をすぐにサポートすることができ、実装の遅れと実装の誤りを回避できました。

デジタル証明書

OS Xではデジタル証明書の使用によって、安全な共同作業がサポートされるとともに、次のセキュリティサービスを利用できます。

- **認証。**デジタル証明書は、作成者または「署名者」が本人であることを保証します。
- **データ整合性。**デジタル証明書によって簡単に署名を行えるようになります。署名を付けることで、メッセージが誤ってまたは悪意によって、変更または改ざんされていないことを確認できます。
- **暗号化。**デジタル証明書によってメッセージを暗号化して、機密情報や個人情報を保護することができます。
- **否認防止。**紙の書類において署名が本人のものであることを証人の署名によって確認できるのと同様、メッセージの受信者は、特

定のメッセージに付された署名が本人のものであることをデジタル証明書によって確認できます。

デジタル証明書の一般的な使用例として、署名付きのEメールやオンラインバンキングがあります。暗号化されたメッセージが受信側に到着すると、受信者の秘密鍵を使ってメッセージが復号化されます。ユーザがデジタル署名付きのEメールを送信するたびに証明書と公開鍵がメッセージに付加され、受信者が暗号化された返信メッセージを送信できるようになります。オンラインバンキングでは、ユーザの銀行に対し、一般に認知されている証明機関（CA）から識別用の証明書が発行されます。このプロセスにより、ウェブブラウザは提示された証明書の有効性を検証し、TLS/SSLを使用した安全なセッションを設定することができ、サイトの識別情報の正当性と、ウェブサイトの通信の暗号化が確認されます。

導入が簡単で拡張性に富んだデジタル証明書は、システム全体に実装され、複数のアプリケーションで共有されています。システム全体にわたるPKIサービスとX.509規格のサポートに加え、OS Xでは開発者がシステム全体にわたる証明書のサポートを利用するための一連のアプリケーションプログラミングインターフェイス（API）を提供しています。

デジタル証明書は、たとえば次のようなOS Xのテクノロジーで使用できます。

- 「FileVault」/暗号化されたディスクイメージ
- ログインウインドウ
- スクリーンセーバ
- 「Safari」（TLS/SSL）
- 「Mail」（S/MIME）
- リモートアクセス（VPN and 802.1X）
- システム管理
- リモートログイン（SSH）
- キーチェーン

OS Xには、小規模な環境や暫定的な環境、あるいは個人向けに、証明書の要求、発行、検証、管理を支援する、軽くて使いやすい証明書アシスタントユーティリティが用意されています。証明書アシスタントは、商用の認証機関（CA）が持つ多くの機能を含め、証明書を作成、管理、発行するためのすべての機能を備え、しかも無償で利用できます。証明書アシスタントによって作成される証明書は、X.509に完全に準拠しているので、暗号化されたEメールの送信、保護されたウェブサイトへのログインなどの数多くの作業をはじめとする、あらゆるPK対応のサービスで使用できます。OS Xは商用CAまたはネットワークCAによって発行された証明書もサポートします。

システムレベルのキーチェーン

OS Xには、ユーザ別のキーチェーンに加えて、システムレベルのキーチェーンも用意されています。このキーチェーンには、ユーザ固有の認証アセット（ワイヤレスネットワーク認証、802.1xネットワーク認証、どこでも My Macサービスなど）は格納されず、信頼されたネットワークサービスの特定に使用される追加の証明書を保存する認証アセットが格納されます。

システムレベルのキーチェーンを変更できるのは、ローカル管理者のみです。「システムルート」キーチェーンには、Appleが発行するルート証明書を保存する変更不可のストアが含まれています。これは管理者が項目の追加や削除の権限を持たない唯一のキーチェーンです。ただし管理者はそれらのルートCA証明書の信頼関係を変更することはできます。

キーチェーン

OS Xの認証情報ストアは「キーチェーン」と呼ばれます。これは、X.509 ID、ユーザ名とパスワード、暗号化キー、秘密メモなど、様々な認証情報を保存する便利で安全なリポジトリです。セキュリティ上は、リソースごとに別のパスワードを使用することが望ましい方

法ですが、ほとんどのユーザにとっていくつものパスワードを覚えることは不可能です（その結果、多くのユーザがユーザ名とパスワードの組み合わせを紙に書いて、机の見やすいところに貼り付けることになります）。キーチェーンは、ユーザの認証情報を管理するための安全なソリューションを提供します。

OS Xのキーチェーンサービスを使用すると、ユーザはファイルサーバ、FTPサーバ、ウェブサイト、Macアカウント、Eメールアカウント、暗号化されたファイルなどの、シングルサインオンに対応していないパスワード保護されたリソースに対して自動的に認証できます。キーチェーンを使用すれば、ユーザはリソースごとの認証情報の入力が不要になり、認証情報を覚える必要さえなくなります。

自動認証用にキーチェーンに保存する項目は、ユーザが選択できます。セキュリティ保護されたリソースにアクセスすると、認証情報を後で使用できるように認証情報を保存するかどうかを尋ねるメッセージが表示されます。保存しない場合は、それ以降、関連のサービスへのアクセス時に、認証情報を再入力する必要があります。キーチェーンが既にロック解除されて利用可能であっても、キーチェーンサービスが追加の認証のために認証情報の使用許可を求めるには、特定のアプリケーションが必要な場合があります。

また、キーチェーンを使用して秘密メモを保存することができます。秘密メモは、ユーザがATMやクレジットカードの暗号番号など、他の形式の秘密情報を格納するために作成するメモです。ユーザは、たとえば、仕事用のキーチェーンと個人のオンラインショッピング用のキーチェーンというように、複数のキーチェーンを作成して、目的の異なる認証情報を保存することができます。キーチェーンはコンピュータ間でコピーできます。

キーチェーンに保存されたすべての個人データは、168ビットトリプルDES（Digital Encryption Standard）を使って保護されます。さらに保護を強化するため、OS Xはログアウト時にユーザのキーチェーンをロックします。ユーザはシステムのスリープ時や一定時間操作がない場合にキーチェーンがロックされるようにOS Xを設定しておくことができます。またいつでも手動でキーチェーンをロックできます。

ユーザのホームディレクトリがネットワークサーバ上にある場合も、すべてのキーチェーン情報はアプリケーションまたはOS Xが要求した場合に、ローカルのクライアントシステム上でのみ復号化されます。キーチェーンに保存された認証情報が暗号化されずにネットワーク送信されることはなく、各ユーザのキーチェーンは安全に保護されます。

コード署名およびアプリケーション署名

アプリケーションにデジタル署名を行うと、アプリケーションの識別情報と整合性が検証され、誤ってまたは悪意によって変更されていないことが確認されます。OS Xが提供するすべてのアプリケーションはAppleが署名します。Mac対応のサードパーティ製ソフトウェアは、開発会社が署名することができます。これはそのソフトウェアがアプリケーションバンドルであっても、Unixバイナリであっても同じです。

アプリケーション署名は、それ自体は本質的な保護を提供しませんが、他のOS X機能と統合することでセキュリティが強化されます。デジタル署名は、たとえばペアレンタルコントロールやクライアント管理プロファイル、「キーチェーンアクセス」アプリケーション、アプリケーションレイヤーのファイアウォールなど、使用しているアプリケーションが、適正で変更されていないバージョンであることの確認が必要な機能で使用されます。

OS Xでは、アプリケーション署名をクライアント管理プロファイル、アプリケーション制限、ペアレンタルコントロールとともに使用すると、アプリケーションの名前を変更したり、元のインストール場所から移動したりしても、ユーザは無許可のアプリケーションを開くことはできません。アプリケーション署名を「キーチェーンアクセス」とともに使用すると、キーチェーンの認証情報を使用するアプリケーションの識別情報と整合性が自動的に検証されるので、表示されるダイアログの数が減少します。アプリケーションレイヤーのファイアウォールとともに使用すると、ネットワークアクセスを許可または禁止されたアプリケーションの整合性が、署名によって特定されて検証されます。アプリケーションレイヤーのファイアウォールとともに使用すると、未署名のアプリケーションが暫定的に署名されます。これにより、アプリケーションが一意に特定され、変更されていないことが確認されます。

ファイアウォール

ファイアウォールの基本的な目的の1つに、ネットワーク上の他のコンピュータやデバイスからコンピュータへの接続を制御することがあります。ほとんどの場合、ファイアウォールソフトウェアの設定には、各アプリケーションがそのアプリケーションのネットワーク接続の制御に使用するネットワークポートやプロトコルに関する知識が必要です。OS Xには内蔵のファイアウォール機能が搭載されています。一時的なユーザ用にはアプリケーションレイヤーのファイアウォールが提供され、より複雑なニーズを持つIT担当者用には業界で定評のあるIPFW2ファイアウォールが引き続きサポートされています。IPFW2ファイアウォールは、通信スタックの最下位であるパケットレベルで管理されます。

アプリケーションレイヤーのファイアウォール

アプリケーションレイヤーのファイアウォールでは、ユーザがポート単位やサービス単位ではなく、アプリケーション単位で接続を制御できます。またファイアウォールは、アプリケーションコード署名によってこの制御の整合性を確保します。このアプローチは、経験の少ないユーザでも簡単にファイアウォールによる保護を利用することができます。また正当なアプリケーション用に開いたポートが、別の不正なアプリケーションによって制御されるのを防止します。

アプリケーションレイヤーのファイアウォールは、アプリケーションで一般に使われているインターネットプロトコルであるTCPとUDPの両方に適用されます。ユーザは「詳細」設定の「ステルスモード」を有効にして、受信ICMP（Internet Control Message Protocol）の「ping」をブロックするようにファイアウォールを設定できます。ステルスモードは、一方的な通信や要求に単に応答しないことによって、プローブサービスからMacを認識できないようにします。

OS Xのデフォルト設定では、ファイアウォールのリストにあるアプリケーションだけでなく、システムが（コード署名の目的で）信頼するCAによってデジタル署名されているすべてのアプリケーションも、外部からの接続を受信できます。Appleの開発によるすべてのアプリケーションは、Appleによって署名されるので、設定を変更せずに外部からの接続を受信できます。デジタル署名されたアプリケーションへのアクセスを拒否する場合は、アプリケーションレイヤーのファイアウォールのリストにそのアプリケーションを追加し、明示的にアクセスを拒否します。

署名がなく、アプリケーションレイヤーのファイアウォールのリストに含まれていないアプリケーションが初めてネットワーク接続を試みた場合、そのアプリケーションの接続を許可するか拒否するかを選択するダイアログが表示されます。ユーザが「許可」を選択すると、OS Xはそのアプリケーションに署名し、アプリケーションファイアウォールリストに自動的に追加します。ユーザが「拒否」を選択すると、OS Xはそのアプリケーションに署名し、アプリケーションレイヤーのファイアウォールのリストに自動的に追加して一切の接続を拒否します。

一部のアプリケーションでは、コード署名を使用せずに、実行時に独自の整合性チェックが行われます。アプリケーションレイヤーのファイアウォールがそのようなアプリケーションを認識した場合、署名は行われず、アプリケーションを実行するたびにOS Xによってダイアログが表示されます。ユーザは、アプリケーションを開発者の署名が入ったバージョンにアップグレードすれば、毎回ダイアログが表示されるのを回避することができます。

アプリケーションレイヤーのファイアウォールでアプリケーションに対するルールが作成されても、その後アプリケーションが変更されると、そのアプリケーションへの外部からのネットワーク接続を許可するか拒否するかを選択するメッセージが再度表示されます。アプリケーションが自動的に変化することはほとんどないので、この安全機能はアプリケーションが変更されたことをユーザに警告するのに役立ちます。

次のような一部の重要なシステムサービスは、アプリケーションレイヤーのファイアウォールの設定と関係なく、外部からの接続を受信できます。

- **DHCP**—DHCP（Dynamic Host Configuration Protocol）やその他のネットワーク構成サービスをサポートするサービス
- **Bonjour**—Appleが提供する設定不要の自動ディスカバリサービス
- **IPSec**—VPN接続の有効化と管理を実行するサービス

IPFW2ファイアウォール

Appleは、ファイアウォールの詳細なルール設定が必要な組織に対応して、UNIXベースのIPFW2ファイアウォールテクノロジーをOS Xに搭載しました。IPFW2は、ネットワークスタック内でアプリケーションレイヤーのファイアウォールよりも下位にあるパケットレベルでトラフィックを処理するので、IPFW2で設定したルールが常に優先されます。アプリケーションレイヤーのファイアウォールとIPFW2ファイアウォールの両方を有効にした場合、アプリケーションレイヤーのファイアウォールは、IPFW2を通過した要求のみを処理します。

コアセキュリティ

OS Xは、ローカルデータとネットワークアクセスの保護に加え、オペレーティングシステムとアプリケーションのコア機能を保護するためのいくつかの機能を備えています。このような機能には、強制アクセス制御、サンドボックス、実行の無効化（XD）機能、ライブラリのランダム化、ヒープメモリの保護、アドレス空間レイアウトのランダム化（ASLR）、アプリケーションの隔離などがあります。これらすべてのサービスを組み合わせて、マルウェアに対する内蔵の階層型防御が形成されています。

強制アクセス制御

OS Xは、強制アクセス制御という、強力で詳細なアクセス制御メカニズムを備えています。この制御では、明示的にアクセスを許可されたプロセスのみがリソースを使用できるように、システムリソース（ネットワーク接続、ファイルシステム、プロセス実行など）へのアクセスが制限されます。強制アクセス制御は、ユーザが直接認識できる機能ではなく、OS Xの複数の防御機能（サンドボックス、ペアレンタルコントロール、プロファイル、「Time Machine」の「セーフティネット」機能）の基盤となるテクノロジーです。

強制アクセス制御とユーザ権限モデルの違いがよく表れているのは、「Time Machine」です。「Time Machine」バックアップに含まれているファイルを削除できるのは、「Time Machine」に関連するOSサービスだけです。ユーザは、「Time Machine」バックアップに含まれているファイルをコマンドラインで削除したり変更したりすることはできません。これは、ルート権限を持つユーザも同様です。

強制アクセス制御は、execシステムサービスと統合され、不正なアプリケーションの実行を阻止しています。これは、ペアレンタルコントロールおよびプロファイルによるアプリケーション制限の両方でアプリケーション制御の基盤となっています。

OS Xのサンドボックス機能（以下を参照）では、システムリソースへのアクセスを強制アクセス制御によって制限します。制限の内容は、サンドボックス化されたアプリケーションごとに提供される特殊なサンドボックスプロファイルによって決まります。つまり、ルートとして実行しているプロセスであっても、システムリソースには「最小権限」と呼ばれるきわめて限定的なアクセスしかできません。

サンドボックス

サンドボックスは、アプリケーションが意図した処理しか実行されないように制限します。これは不正なコードがアプリケーションやオペレーティングシステムサービスをハイジャックして、独自のコードを実行しないように防止するのに役立ちます。この目的を達成するために、サンドボックスではアプリケーションを統制して、アプリケーションがどのファイルにアクセスできるか、アプリケーションがネットワークと通信できるかどうか、アプリケーションを使ってほかのアプリケーションを起動できるかどうかを制限します。OS Xでは、ネットワークと日常的に通信するシステムヘルパーアプリケーションの多くがサンドボックス化され、システムにアクセスしようとする攻撃者の不正行為から保護されています。このようなア

プリケーションには、mDNSResponder（Bonjour の基盤になっているサービス）、configd（DHCPおよびネットワーク設定を提供）、Kerberos KDCなどがあります。信頼されていない入力（任意のファイルやネットワーク接続など）を定期的に受け付けるその他のプログラムもサンドボックス化されています。たとえば、Xgrid、クイックルック、Spotlightのバックグラウンドデーモンなどです。

実行の無効化

不正なソフトウェアの開発者が、システムに不正アクセスするためによく使うテクニックの1つに「バッファオーバーフロー」があります。バッファオーバーフローは、ソフトウェア開発者が、任意の長さの入力に対して、誤って固定量のメモリをバッファとして割り当てた場合に発生します。

たとえば、プログラムがファイル名などのテキスト文字列を処理し、ファイル名は256文字以下いう想定の下にプログラムにファイル名が書き込まれるとします。ファイル名を表す文字列のバッファが256文字の固定長で、それより長い入力がバッファに与えられた場合、入力がバッファをオーバーフローします。

システムをハイジャックしようとするソフトウェアは、バッファオーバーフローのような脆弱性を利用して、悪意のある独自のコード（一般にシェルコードと呼ばれます）を実行することができます。OS Xは、Intelプロセッサ搭載システム対応版のリリース以降、新型Intelマイクロプロセッサが持つXD機能を利用した実行不可スタック保護を提供してきました。XDを使用すると、ソフトウェアのオブジェクトコードへのコンパイル時に、コンパイラがプログラムの特定の領域をデータ専用の格納領域としてマークします。これにより、プロセッサはデータ専用に指定された領域で命令を実行しなくなります。

ライブラリのランダム化

実行の無効化機能はバッファオーバーフローを利用した攻撃から防御する手段を提供しますが、これに対し、「return to libc」と呼ばれるよく知られた手法はスタックXDを迂回します。「return to libc」攻撃では、スタック上の正しいリターンメモリアドレスを、システム関数の既知のメモリアドレスに置き換えます。この手法の名前は、システムのCライブラリ（libc）にあるsystem()などの関数を呼び出すことが多いことから「return to libc」と名付けられています。

OS Xでは、システムのインストール時やシステム上でライブラリのプレバインドが更新されたときに、システムのライブラリ読み込みアドレスがランダムに生成されます。このランダムなアドレス生成は、通常、システムソフトウェアのアップデート後に実行されますが、次のコマンドを実行して強制的にアップデートすることもできます。

```
update_dyld_shared_cache -force
```

いずれのMacでも、システムアップデートから次のシステムアップデートまでの間、特定のライブラリ関数のアドレスは、数千というランダムな位置の1つに固定されます。しかしすべてのMacシステムを考えると、1台のMac上の特定のライブラリのアドレスは、別のMacの同じライブラリのアドレスとは異なります。このランダム化に

よって、OS Xが動作する特定のMacで、システムライブラリ関数のアドレスを知ることが難しくなるので、「return to libc」攻撃がはるかに困難になります。

アドレス空間レイアウトのランダム化

アドレス空間レイアウトのランダム化（ASLR）は、システムライブラリのランダム化と同様、攻撃者がターゲットのアドレスを予測することを、不可能ではないにせよ困難にすることにより、一部のタイプのセキュリティ攻撃から防御します。大容量の64ビットアドレス空間を使用することで、ランダムオフセットのエントロピーが増大します。ASLRは、たとえば「return to libc」やシェルコード注入などのターゲットを絞った攻撃に対する防御を強化します。

マルウェア防止

ネットワーク内のデータ、ワークステーション、サーバを保護する方法は、暗号化とアクセス制御だけではありません。共同作業と文書共有に対するニーズが高まるにつれ、ユーザが自分でも知らないうちに、悪意のある実行可能コードが潜む文書やファイルを受け入れ、さらには共有する可能性が生じています。OS Xでは一般に、ウイルスやその他の形態のマルウェアに感染するリスクは高くありませんが、OS Xに影響を及ぼす可能性のあるいくつかの形態のマルウェアが発見されていることは事実です。

アプリケーションの隔離

OS Xでは、Macにダウンロードされるすべての実行可能コードは、それが隔離されていることを示すファイルシステムレベルの拡張属性およびメタデータ（ZIPアーカイブまたはディスクイメージのいずれかの形式で配布された場合は、それらの形式からファイルシステムに伝搬されます）によってタグ付けされます。OS Xは、初めてコードを実行する前にユーザの同意を求めるとともに、コードがダウンロードされた日時、ダウンロードに使用されたアプリケーション、現在配置されている場所、またコードがウェブからダウンロードされた場合は、ダウンロード元のURLをあわせて表示します。アプリケーションを隔離することで、ユーザやプロセスが未知の提供元から入手した、悪意がある可能性を持つアプリケーションを誤って実行することを防止できます。

隔離機能を利用するように作成されているアプリケーション（「Safari」や「Mail」など）は、インターネットからダウンロードされたファイルや、Eメールの添付ファイル、様々なリムーバブルメディアやファイルサーバ上の共有ポイントでアクセスするファイルに対して、追加の防御レイヤーを備えることになります。隔離機能によって、インターネット関連のアプリケーションは、そのようなファイルに隔離属性を追加できます。

隔離属性を持つアプリケーションを開くと、アプリケーションを起動するかどうかを尋ねるメッセージがOS Xによって表示されます。ユーザが承認した場合、OS Xは隔離属性を除去し、通常どおりにアプリケーションを起動します。

マルウェアの識別と削除

未知の実行可能コードがMacにダウンロードされると、OS Xが持つ別の保護機能が、ユーザの管理作業なしに動作し、コードが既知のマルウェアである場合にそのコードが実行されないようになります。マルウェアの可能性のあるコードは既に隔離されているので、OS Xは即座にそのマルウェアを削除し、ユーザに対し、悪意のある試みが阻止されたことを通知します。マルウェアを識別する方法には、パターン照合やシグネチャー照合、既知のペイロードの識別、名前付け規則などがあります。マルウェアに対するこの追加の防御レイヤーを維持するため、シグネチャー照合などの識別に使用する定義は、毎日自動的にアップデートされます。

ウイルス対策保護

大規模組織の多くは、ウイルス除去プロセスとして、まずメールサーバを通過するすべての送受信メールをスキャンします。どのサーバプラットフォームを使用する場合も、境界でのウイルスのスキャンと捕捉によって、ウイルスがユーザのデスクトップにたどり着く可能性は大幅に低下します。今日、従業員が自宅で文書を作成するために、ポータブルコンピュータやその他のポータブルデバイスをエンタープライズネットワークの外に持ち出すことはよくあります。従業員のシステムに無料のまたは市販のウイルス対策ツールをインストールし、Windowsのみを対象とするウイルスを含め、従業員がマルウェアを拡大させないように自社ネットワーク外でも防御策を講じることを検討してください。

組織内で、一元管理によってOS Xシステムにウイルス対策を導入すると、ウイルス対策ソフトウェアと定義を常に最新の状態に保つことができます。また一元的なウイルス対策管理を使用して、管理者に対し、個別のマシンにウイルスが存在することを警告できます。エンタープライズ環境にあるMacシステムの一元的ウイルス対策管理ソリューションは、多くのエンドポイント保護ベンダーから提供されています。

プライバシー

モバイルデバイスやモバイルアプリケーション、クラウドサービスの急速な普及に伴い、個人情報保護の意識を向上させる必要性が高まっています。マッピングサービスを使って目的地までの地図を表示させたり、現在地からの詳細な道順を説明させたりするには、デジタルデバイスが正確な位置情報を提供できる必要があります。しかし詳細な位置情報を提供することで、許可を与えていないサービスやアプリケーションに個人情報や機密情報が渡ってしまうことがあります。

位置情報サービス

OS Xには環境設定を制御する機能があり、ここで位置情報サービスを制御できます。OS Xの「セキュリティ」環境設定にある「プライバシー」ペインでは、位置情報サービスの有効と無効の切り替えや、診断データや使用状況データの収集を1箇所で実行できる場所です。ユーザはこの「プライバシー」ペインを使って、位置情報にアクセスできるアプリケーションを管理できます。

オンラインプライバシー

OS X 「Safari」の環境設定にある「プライバシー」ペインでは、オンラインプライバシーに関する詳細情報が表示され、オンラインプライバシーを制御することができます。ユーザは、ウェブサイトのデータの消去やcookieの設定のカスタマイズのほか、ウェブサイトから位置情報を要求できるかどうかを決定できます。「Safari」の「プライバシー」ペインにはまた、Macにデータが保存されているすべてのウェブサイトのリスト、各サイトによって保存された情報、情報が保存されているシステム上の場所のリストが表示されます。「Safari」では、ウェブサイトがユーザのオンラインアクティビティの追跡に使用する情報を簡単に消去できます。またcookieやFlashのプラグインデータ、さらにはデータベース、ローカルストレージ、アプリケーションキャッシュなどの情報を完全に消去できます。これらのリポジトリの情報は、サイト単位で指定して消去することもできます。

結論

セキュリティは、すべてのIT部門にとって絶えず存在する懸念事項です。OS Xが提供する充実したセキュリティコンポーネントのセットは、すべてのMacに内蔵され、業界標準のソリューションを統合し、米国連邦政府機関の厳格なセキュリティガイドラインに適合するかそれを超えた性能を備えています。このような要素をすべて兼ね備えたMacは、あらゆる組織のIT基準を満たします。

03-29-2012