クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－

蔭山 哲也　鈴木 亮生

要 旨

企業の情報漏えいに対する防止対策として、企業内の電子ファイルを暗号化するSaaS型サービスであるクラウドセキュアファイルサービスについて紹介します。本サービスは、ファイル暗号化製品である「InfoCage FileShell」をベースにしたサービスです。管理サーバ機能をクラウド上で提供し、Microsoft社のAzure Information Protectionサービス及び企業ユーザー側でインストールしたクライアントと連携してDRM技術に基づくファイル暗号化をサービスとして提供します。従来の個別システムではカスタマイズの自由度はあるものの、ポリシーを設計し管理サーバを構築運用する負担がありました。NEC社内での運用ノウハウをポリシーとして提供し、構築済みのクラウド環境を提供することで、企業ユーザーに容易に利用可能なサービスとして提供するものです。

KeyWords

セキュリティ／情報漏えい対策／ファイル暗号化／クラウド／サービス

1. はじめに

独立行政法人 情報処理推進機構（以下、IPA）が発行した2017年度版「情報セキュリティ10大脅威」において、1位と5位に情報漏えいに関する脅威がランクインしています。なかには情報漏えいによって業務が停止してしまう事例も見られ、社会的影響も拡大しています（**表**）。

また、これら組織の情報漏えい事案のほとんどが「標的型攻撃」「内部不正」に起因して発生し、標的型攻撃の高度化をはじめ、改正個人情報保護法への対応など、組織の機密情報（技術情報、個人情報）の漏えいのリスクはますます高まり、経営上のリスクも拡大しています。

表　情報セキュリティ10大脅威（IPAより）

2016年順位	2017年順位	組織の脅威
1位	**1位**	**標的型攻撃による情報流出**
7位	2位	ランサムウェアによる被害
3位	3位	ウェブサービスからの個人情報の窃取
4位	4位	サービス妨害攻撃によるサービスの停止
2位	**5位**	**内部不正による情報漏えいとそれに伴う業務停止**
5位	6位	ウェブサイトの改ざん
9位	7位	ウェブサービスへの不正ログイン
ランク外	8位	IoT機器の脆弱性の顕在化
ランク外	9位	攻撃のビジネス化（アンダーグラウンドサービス）
8位	10位	インターネットバンキングやクレジットカード情報の不正利用

NECでは、2010年から情報漏えい防止の対策として、ファイル暗号化ソフト「InfoCage FileShell」を販売し情報漏えい対策を提供しており、NEC社内はもとより、合計のべ50万人の利用実績があります。そして今般、その「InfoCage FileShell」をベースに、NECのセキュリティサービスであるActSecureからSaaS型セキュリティサービス「クラウドセキュアファイルサービス」として販売を開始しました。

2.「InfoCage FileShell」の仕組みと課題

本サービスのベース製品である「InfoCage FileShell」は、デジタル著作権管理技術（Digital Rights Management：DRM）を使い永続性のあるファイル保護を実現するソフトウェア製品です。具体的には、Microsoft社（以下、MS社）のRMS（Rights Management Services）を利用し、Windows環境でDRM基盤を提供します。MS社のRMSを利用する文書保護機能としては、同じMS社のOffice IRM（Information Rights Management）があります。FileShellでは、Office IRMに対し以下のように機能拡張を可能にし、利用者が特別な操作を意識することなく、

ファイル保護機能を実現する仕組みを提供します（**図1**）。

- Microsoft Office以外のアプリケーションへの対応
- 組織内で統一した保護ルールを徹底（統制環境の提供）
- 文書管理サーバと連携した、文書の保護
- 個人ローカル環境に散在するファイル群に保護ルールを自動適用
- 拡張されたログの提供

「InfoCage FileShell」により、ファイル保護を実現するには、お客様のネットワーク内に管理系サーバ環境の構築が必要です。そのため、その環境を構築・運用可能な中～大企業のお客様で採用いただいていました。しかし、情報漏えいの脅威は企業規模にかかわらず発生します。NECは、「InfoCage FileShell」で実現可能なファイル保護の仕組みを広くさまざまなお客様に利用いただくため、「InfoCage FileShell」をベースにしたSaaS型セキュリティサービスの開発を行い、2017年6月に販売を開始しました（**図2**）。

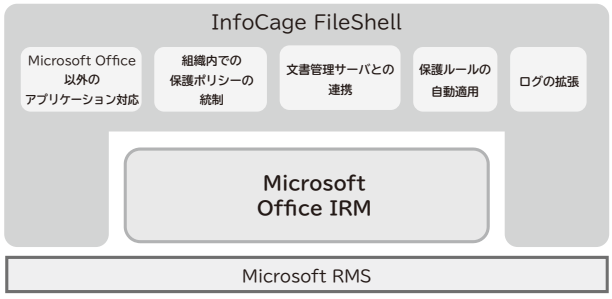


図1　InfoCage FileShellとMicrosoft RMSの関係

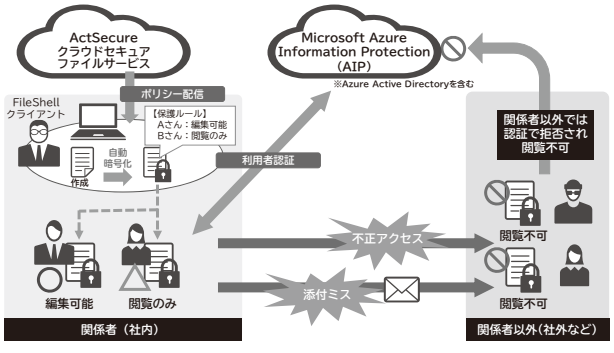


図2　ActSecureクラウドセキュアファイルサービス概要

3. サービスの技術的特長

本サービスの特長であり、「InfoCage FileShell」製品との違いは3点あります。

- お客様環境での管理系サーバ群の構築が不要
- 認証基盤としてAzure Information Protection（AIP）を採用し、サービスに含み提供
- NEC社内利用ノウハウによる管理ポリシー

まず1点目は、本サービスを利用いただくことで、「InfoCage FileShell」導入時に必要となる管理系サーバ群（管理サーバ、RMSサーバ、データベース）を、お客様が準備する必要がなくなります。この特長により、導入までの期間の短縮や、サーバ導入に関するコスト、サーバ運用に関する人的負担を低減することができます。

2点目は、本サービスでは「InfoCage FileShell」が認証基盤として利用するMicrosoft RMSをサービスに含んで提供します。したがって、1点目同様、お客様がサービス利用のために環境構築や、その管理を行う必要はありません。

3点目は、NEC自身が「InfoCage FileShell」を導入し情報漏えい対策として運用しており、その運用ノウハウをサービスにフィードバックしています。具体的には、運用時に必要となるファイルの保護ポリシーをあらかじめサービスで用意し、そのルールに則っていただくことでポリシー作成の負担を低減しています。

以下、各特長の詳細を説明します。

3.1 FileShellサーバのクラウド提供

「InfoCage FileShell」は、エージェントと、それを管理する管理サーバで構成されます。管理サーバは、クライアント管理機能及びデータベースにて構成されます。クラウドサービス化に伴い、管理サーバをお客様ネットワーク内に設置することが不要となりました。更に複数企業ユーザーで共用可能なサービス提供機能についてはクラウド上で統合するなど、サービス全体で効率的に集中、統合管理するようシステムを構成しています。

「InfoCage FileShell」はMS社のRMSと連携して動作しますが、本サービスではその代替として、同じくMS社のAIPを利用して実現しています。AIPはクラウドサービスであるため、RMSサーバも構築不要としています。AIP以外の管理系サーバは、NECのクラウドサービ

ス基盤NEC Cloud IaaSを使い、安全性・可用性・効率に配慮して構築しています。

また、このサービス基盤はNEC内で定められたセキュア運用・セキュア開発ガイドラインに準拠し、システム構成、設定に加え、定期的な、セキュリティ診断なども併用することで、安全・安心なサービスの設計構築を行っています。

3.2 Azureとの連携のポイント

前述のように、本サービスでは認証基盤として、MS社のAIPを採用しており、サービスに含めて提供します。必要事項を申請いただく以外に、Azureの設定を含め、いっさいお客様側での手配は必要ありません。AIPでは認証のためにIDパスワード入力が必要ですが、ファイルへのアクセスのたびにAzureの認証が発生しないよう、代理認証（シングルサインオン）の仕組みをあらかじめ導入し、お客様の利用負荷を低減し安全なファイル暗号化環境を提供しています。

3.3 NECの運用ノウハウをサービスに

「InfoCage FileShell」は、導入時にファイルを暗号化する場合の取り扱い（保護対象拡張子、自動暗号化対象フォルダ、制御アプリケーションなど）などのポリシーをお客様の部門・組織に応じてカスタマイズすることが可能です。しかし、サービス化にあたっては、多くのお客様に安全かつ効率良く利用いただくため、設定の柔軟性及びお客様固有システムとの連携機能を限定する形で、単一のポリシーでシンプルに提供しています。このポリシーは、NEC社内での十数万台の運用経験や、50万IDに「InfoCage FileShell」を販売してきた経験をもとに、お客様で利用されるOSや環境を広くサポートできるようにポリシーを定義し、幅広いお客様に利用いただけるポリシーとしています。

クラウドセキュアファイルサービスポリシー

- 契約企業単位で一つの暗号化ポリシーのみ利用可能
- クライアントの役割を３種類に限定
  - 暗号化解除も可能な特権管理者
  - 暗号化解除以外の操作が可能な一般利用者
  - ファイル閲覧のみ可能な限定利用者

パブリックサービスでは、個々のお客様の個別要望をすべて満たすことはもとより不可能ですが、これまでの運用・販売の経験から、多くのお客様が許容可能なポリシーを定義し提供しています。

4. クラウドサービスの安全な運用のために

クラウド提供においてはお客様ごとの利用条件を申請いただき、お客様個別情報を持つクラウド環境を提供します。お客様の変更要望への対応あるいは、お客様の問い合わせに対しては、変更作業の実施及びその回答を行う窓口を設けています。更に、万一クラウド環境で障害が発生した場合に備えて、日々機器を監視し、問題があった場合には、速やかにお客様に通知して回復に努める体制を保持しております。これ以外にも随時最新のセキュリティ対策情報を収集するなど、インターネット上で機能を提供するための必要な業務を実施しています。また、クラウドサービス化にあたり、お客様から申請いただいた利用ID数の確認機能や、クライアントと定期的に通信を行う機能を追加し、安全に安定したサービス提供を実現しています。

5. 今後の展開

ActSecureクラウドセキュアファイルサービスにおいては、「InfoCage FileShell」で実現している機能の追加を予定しています。また、お客様環境個別のポリシーの許容する上位サービスなど、今後もサービス強化を進めていく予定です。

ActSecure SaaS型セキュリティサービスでは、今回説明しましたクラウドセキュアファイルサービス以外にも、メールのスパム対策・ウイルス対策・標的型攻撃対策・誤送信防止などの送受信機能を持つクラウドメールセキュリティサービス、Webサーバをアプリケーション層で防護するクラウドWAF（Web Application Firewall）

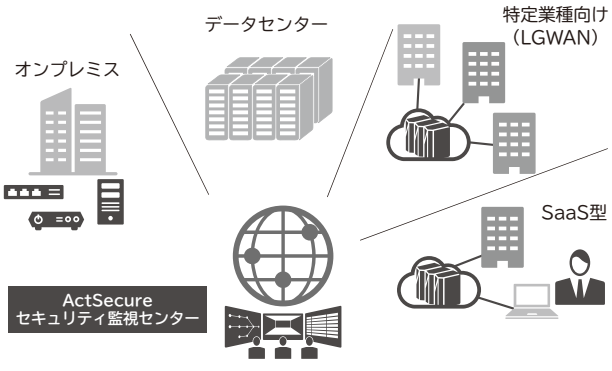


図３　ActSecureトータルセキュリティサービス

サービス、UTM（Unified Threat Management）製品のサンドボックス機能をリモート提供するクラウドサンドボックスサービス、DDoS（Distributed Denial of Service Attack）攻撃に対する防御を行うクラウドDDoSサービスなどを既に提供しています。

企業のセキュリティ対策においては、インターネットとの通信経路、機器監視などに加え情報の取り扱い、企業内セキュリティ管理、インシデント対応などさまざまな場面が存在します。今後もActSecureトータルセキュリティサービスとして企業のセキュリティ対策に役立つ各種サービスを随時提供していく予定です（**図3**）。

参考文献

1）情報処理推進機構：情報セキュリティ10大脅威 2017, 2017.5
https://www.ipa.go.jp/security/vuln/10threats2017.html

執筆者プロフィール

蔭山 哲也
スマートネットワーク事業部
マネージャー

鈴木 亮生
スマートネットワーク事業部
シニアエキスパート

関連URL

InfoCage FileShell
http://jpn.nec.com/infocage/fileshell/

クラウドセキュアファイルサービス
http://jpn.nec.com/act/acts_securefile.html

ActSecureトータルセキュリティサービス
http://jpn.nec.com/act/acts_index.html

NECクラウド基盤サービスNEC Cloud IaaS
http://jpn.nec.com/cloud/service/platform_service/iaas.html

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

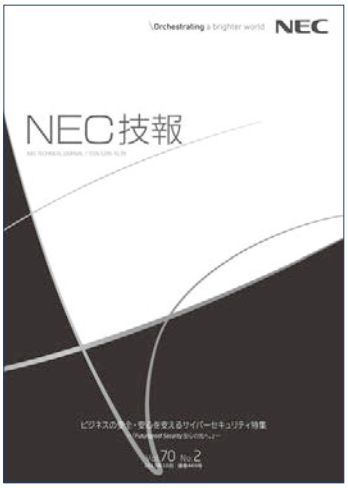
◇ 特集論文

社会の動向とNECの取り組み
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
（2017年10月）

特集TOP