

## アシスト、監視強化や侵害拡大防止を重視した 「標的型攻撃対策ソリューション」を発表

～ 内部対策を重視し、侵入されてもデータを持ち出させない施策を体系化 ～

株式会社アシスト(本社:東京都千代田区、代表取締役社長:大塚 辰男、略記:アシスト)は、標的型攻撃による情報漏洩事件が次々に発生し、マイナンバー制度の施行も10月に控えた今、政府、自治体、企業において大きな関心が寄せられている標的型攻撃への対策を支援するために、内部対策を重視した様々な施策を「標的型攻撃対策ソリューション」として体系化し、本日より提供を開始します。

アシストでは標的型攻撃への対策として、今年5月に、情報漏洩が疑われる不正なインターネット通信やマルウェアの侵入状況を自社で容易に確認できるオリジナル製品「BlackDomainSensor」の提供を開始しています。その他にも、外部からの脅威だけでなく、内部のデータ保護を強化するセキュリティ対策として、共有データの暗号化をベースに、認証強化、ファイル単位の制御を組み合わせることでよりセキュアなデータ利用環境を実現する「ファイルサーバ情報漏洩防止ソリューション」や、特権IDの適切な貸出制御を実現し、不正利用による情報窃取を防止する「特権ID管理ソリューション plus」などを展開してきました。

標的型攻撃の手口は日々巧妙化し、新たな攻撃パターンが次々と発生するため、完全に防御することは不可能とされています。また内部への侵入、外部への持ち出しといった入口・出口対策だけでは対応が後手に回る可能性が高いことから、アシストでは、内部への侵入を前提とし「監視強化」および「侵害拡大防止」など内部対策を重視した多角的な施策を、この度「標的型攻撃対策ソリューション」として体系化し、提供を開始することになりました。

具体的には、マルウェアの侵入の予兆や状況の把握のため定期的なモニタリングを実施する「[BlackDomainSensor](#)」、内部対策として、特権IDを奪取されたとしてもデータを持ち出させない、また持ち出されても意味が無いようにするための多重対策として「マルウェア遮断ソリューション」、「ダブルブラウザソリューション」、「[特権ID管理ソリューション](#)」、「[ファイルサーバ情報漏洩防止ソリューション](#)」の全5ソリューションを展開します。「マルウェア遮断ソリューション」については10月に新設を予定、また「[ダブルブラウザソリューション](#)」については10月に機能強化版の提供開始を予定しています。

アシストは今後も顧客企業・団体の重要な資産である「データ=情報」を保護するための様々なセキュリティ対策の強化に取り組み、ソリューションを展開していきます。

## ■「標的型攻撃対策ソリューション」について

### (1)「BlackDomainSensor」

セキュリティログ分析エンジンを使って、インターネットアクセスログと C&C サーバのリストを突合せた結果と、Active Directory に特権 ID を模したトラップアカウントを仕掛け、おとりに引っ掛かったマルウェアの認証失敗ログを抽出したレポートを出力します。

#### 【対策の有効性】

- ・ マルウェアによる C&C サーバへ通信している端末の発見
- ・ マルウェアによる特権 ID 奪取の挙動を発見

URL : <http://www.ashisuto.co.jp/product/theme/security/blackdomain-sensor.html>

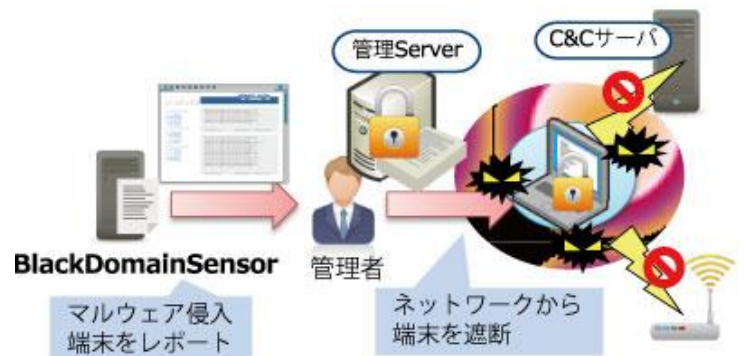


### (2)「マルウェア遮断ソリューション」 ※10月に新設予定

マルウェアが侵入している可能性のある端末をネットワークから遮断します。遮断は管理者がリモートから実施可能です。

#### 【対策の有効性】

- ・ 該当端末の C&C サーバへの不正な通信をブロック
- ・ データの不正な持ち出しや侵害拡大を防止



### (3)「ダブルブラウザソリューション」 ※10月に機能強化版をリリース予定

インターネットアクセス用のブラウザを仮想環境で提供し、業務用端末から外部へのインターネットアクセス(HTTP 通信)を禁止させ、業務用端末のインターネットアクセスを分離します。

#### 【対策の有効性】

- ・ マルウェアが侵入したとしても、標的型攻撃の出口となる C&C サーバとのインターネットアクセスを禁止することで、攻撃を無効化

URL : <http://www.ashisuto.co.jp/product/theme/virtualization/doublebrowser.html>



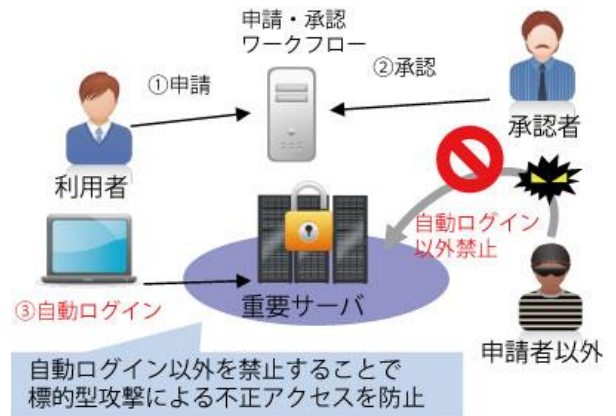
#### (4)「特権 ID 管理ソリューション」

特権 ID はワークフローにて申請を行い、承認された場合のみ利用できるように制御します。また、重要サーバへはワークフロー経由の自動ログインのみを許可し、自動ログイン以外のローカルログイン等はすべて禁止します。

##### 【対策の有効性】

- ・ ワークフローを経由しない重要サーバへのログインを一切禁止することで、万が一標的型攻撃によって特権 ID を奪取された場合でも不正なアクセスを防止

URL : [http://www.ashisuto.co.jp/product/theme/security/privileged\\_identity\\_management.html](http://www.ashisuto.co.jp/product/theme/security/privileged_identity_management.html)



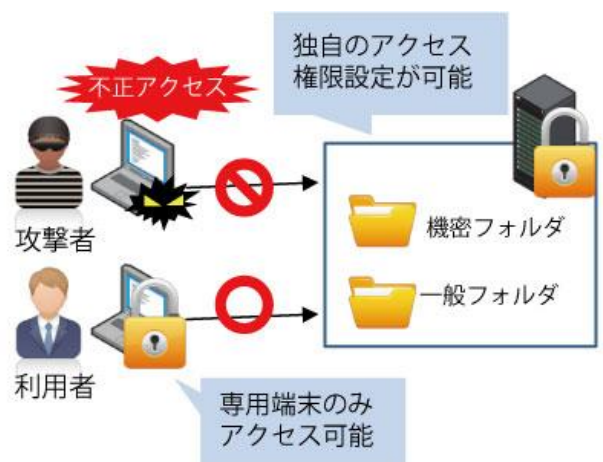
#### (5)「ファイルサーバ情報漏洩防止ソリューション」

ファイルサーバのデータを暗号化し、Windows のアクセス権限とは別に独自のアクセス権を設定。また、ファイルサーバに対してアクセスできるのは、専用クライアントが導入されている端末のみに限定します。

##### 【対策の有効性】

- ・ 独自のアクセス権限設定により、専用端末以外からのデータ持ち出しを防止。Windows の特権 ID を奪取された際も、データの持ち出しリスクを軽減
- ・ 標的型攻撃により、データが直接持ち出された際もデータは暗号化された状態を維持

URL : [http://www.ashisuto.co.jp/product/theme/security/file\\_server\\_leakage.html](http://www.ashisuto.co.jp/product/theme/security/file_server_leakage.html)



#### ■ 関連記事

アイティメディア株式会社の「TechTarget Japan」に、アシストが考える「標的型攻撃への対策方法」について、インタビュー記事が掲載されました。

##### <タイアップ記事>

標的型攻撃対策の現実解、「可視化」と「内部対策」のススメ

<http://techtarget.itmedia.co.jp/tt/news/1508/12/news03.html>

##### <ダウンロード記事>

1.マルウェアは侵入しているのかいないのか？ 標的型攻撃対策の第一歩

<http://wp.techtarget.itmedia.co.jp/contents/?cid=17721>

2.守るべきデータを中心とした「内部対策」に不可欠な2つの要素

<http://wp.techtarget.itmedia.co.jp/contents/?cid=17722>

## ■関連イベント

アシストが考える「標的型攻撃対策ソリューション」の詳細を以下のイベントにて紹介します。

◎タイトル:

アシストテクニカルフォーラム 2015 ビジネス・イノベーションを支えるITへ

概要:

市場の変化をいかに素早くとらえチャンスに変えられるかが、ビジネス成功の鍵となります。本イベントでは、現場で磨かれてきた、ビジネスチャンスを生み出す情報システム構築・運用のエッセンスを紹介します。

日時:2015年10月22日(木) 13:00~18:00 (受付開始 12:30~)

申し込みURL:<https://mp.ashisuto.jp/public/seminar/view/4671>

\* 関連セッション

<情報漏洩対策トラック>

E-1 情報漏洩の脅威とリスクを簡単に見える化できるログ分析

E-2 最強の標的型攻撃対策はこれだ！業務PCのネットからの分離

E-3 情報漏洩対策のために本当に必要な特権ID管理のススメ

<仮想化／セキュリティトラック>

F-1 Ericom Connect徹底解説

F-2 マイナンバー時代のデータベースセキュリティ情報はこうして護る

F-3 情報漏洩からデータを守る！いまだきのエンドポイントセキュリティ

## ■株式会社アシストについて

代表取締役会長:ビル・トッテン／代表取締役社長:大塚 辰男

設立:1972年3月

社員数:870名(2015年4月現在)

本社:東京都千代田区九段北 4-2-1

URL:<http://www.ashisuto.co.jp/>

アシストは、特定のハードウェア・メーカーやソフトウェア・ベンダーに偏らない、幅広いパッケージ・ソフトウェアを取り扱う会社です。「パッケージ・インテグレーター」として複数のソフトウェアと支援サービスにアシストのノウハウを組み合わせ、企業の情報システムを情報活用、運用、データベースを中心に、近年ではクライアント仮想化やビジネスルール管理分野も拡充し支援しています。今年も「お客様の最高」のために”というスローガンのもと、これらの分野にさらに注力し、顧客企業の立場に立った製品選定と独自の組み合わせによる製品／サービスの提供を一層強化し、活動していきます。

## ■ニュースリリースに関するお問い合わせ

株式会社アシスト 広報部 担当:田口、吉田

TEL:03-5276-5850 FAX:03-5276-5895 E-Mail:[press@ashisuto.co.jp](mailto:press@ashisuto.co.jp)

## ■「標的型攻撃対策ソリューション」に関するお問い合わせ

株式会社アシスト システムソフトウェア事業部 担当:彦坂

TEL:03-5276-5565 FAX:03-5276-5879 E-Mail:[ssj\\_news@ashisuto.co.jp](mailto:ssj_news@ashisuto.co.jp)

※ 記載されている会社名、製品名は、各社の商標または登録商標です。

※ ニュースリリースに記載された製品／サービスの内容、価格、仕様、お問い合わせなどは、発表日現在のものです。その後予告なしに変更されることがあります。あらかじめご了承ください。