2012 年 9 月 28 日

「Biz マネージドセキュリティサービス」の新機能提供について

NTT コミュニケーションズ（略称：NTT Com）はグローバルでトータルなセキュリティ対策のアウトソーシングサービス「Biz マネージドセキュリティサービス」において、企業を標的としたサイバー攻撃に対応する新機能として、「ネットワークプロファイリング」「ファイル検査」「DLP[*1]」を 2012 年 9 月 28 日より提供します。

本機能の導入により、未知の攻撃手法やウイルスを検知することで、標的型攻撃などの新たな脅威から自社の ICT 環境を守り、情報漏えいリスクを最小化することができます。更に、他の機能とともにトータルで導入することで、様々なセキュリティログを相関分析し、更に高度な潜在リスクの検知と強固なセキュリティ対策が可能となります。

1.新機能の概要（別紙参照）

(1) ネットワークプロファイリング

お客さまネットワーク上に設置する機器にて通信のセキュリティ監視を行い、不正アクセスやウイルスを検知します。専門アナリストが、従来の IDS[*2]/IPS[*3] のシグネチャーやウイルス対策のパターンファイルでは危険と判定されない通信も分析し、標的型攻撃のような未知の脅威や潜在的なリスクを検出、可視化します。分析結果をもとに危険度を判定し、対応方法についてもレポートします。

本機能の導入により、これまでに危険と判定されなかったネットワーク上のセキュリティリスクに対して、早期発見と適切な対策を実施することができます。

(2) ファイル検査

お客さまネットワーク上に設置する機器にて通信のセキュリティ監視を行い、メールの添付ファイルやインターネットからのダウンロードファイルを解析します。隔離された安全な疑似環境でファイルを試験し、不審な動作をしないかを確認しますので、従来のウイルス対策では発見できないような未知のウイルスを検出できます。

本機能の導入により、未知のウイルスが仕組まれたメールの添付ファイルを使用した標的型攻撃など、新たなセキュリティ上の脅威に対応することができます。

(3) DLP

情報の持出禁止ポリシーを設定したセキュリティ機器（ネットワーク DLP）をお客さまネットワーク上に設置し、持出禁止ポリシーに違反する機密情報などの送信ファイルを検出、通知します。情報漏えいの発生や兆候の発見時には、ファイルの特定や漏えい経路などの追跡を支援します。

本機能の導入により、機密情報の持出制限を社員の判断に委ねず、システマチックにルールを徹底することができます。また、情報漏えいの状況を把握することで、より効果的な対策の検討や社外への影響度を判断することができます。

2. 料金

(1) ネットワークプロファイリング：208,000 円/月

(2) ファイル検査：（Web アクセスセキュリティ）280,500 円/月

（E-mail セキュリティ）599,000 円/月

(3) DLP：241,500 円/月

※上記は、オンプレミス環境における参考月額料金（税込）です。

料金はお客さまのシステム環境により異なり、別途、初期料金が必要です。

3. 提供開始日

2012 年 9 月 28 日(金)

4. NTT Communications Forum 2012 への出展

2012 年 10 月 25 日(木)、26 日(金)にザ・プリンス・パークタワー東京で開催される「NTT Communications Forum 2012」において、「ネットワークプロファイリング」「ファイル検査」「DLP」などのデモンストレーションを実施予定です。

http://www.ntt.com/forum/

*1 Data Loss Prevention の略 機密データを社外へ流出させないための包括的な情報漏えい対策

*2 Intrusion Detection System の略 通信回線を監視し、ネットワークへの侵入を検知して管理者に通報するシステム

*3 Intrusion Prevention System の略 サーバやネットワークへの不正侵入を阻止するツール

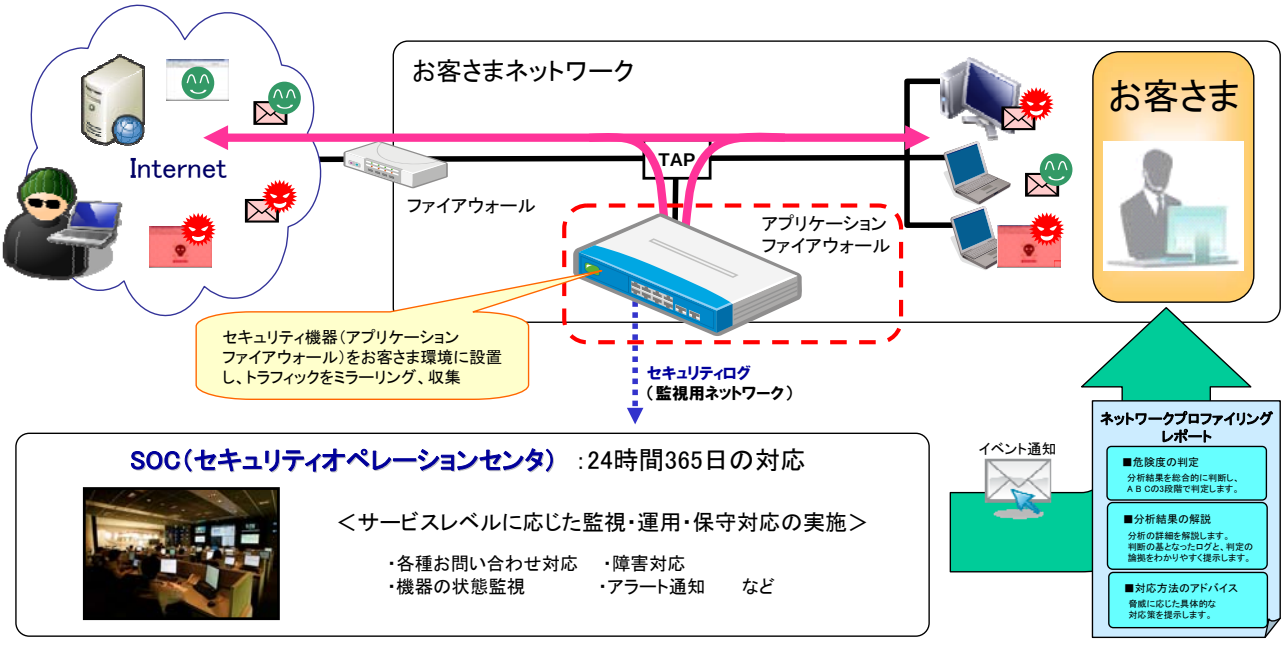
別紙　「Bizマネージドセキュリティサービス」のメニュー

カテゴリ	メニュー	サブメニュー	概要	運用レベル *2 1	2	3	参考料金（税込） *3
リスクモニタリング	脆弱性診断	ネットワーク/アプリケーション脆弱性診断 脆弱性マネジメント	お客さま環境の脅威に対する対策（パッチ適用など）の十分性を可視化し、確認	－			ネットワーク脆弱性診断 1,010,500円 アプリケーション脆弱性診断 971,500円 脆弱性マネジメント 1,522,500円／月 *4
	プロファイリング（セキュリティレポート）	ネットワークプロファイリング *1	お客さま環境（ネットワーク、サーバー）における通信状況を分析し、未知の脅威、潜在リスクの有無を可視化	◎	－	○	208,000円／月 *4
		アプリケーションプロファイリング	お客さま環境における利用中のアプリケーションの通信状況を分析し、未知の脅威、潜在リスクの有無を可視化				208,000円／月 *4
不正アクセス&ウイルス対策	ネットワークセキュリティ	Firewall	ネットワーク上を流れる脅威（不正な通信およびウイルス）を検知し、防御	◎		○	196,500円／月 *4
		IDS/IPS					222,000円／月 *4
	Webアクセスセキュリティ	ウイルス対策（Web）	Webサイトとの通信における脅威（不正な通信およびウイルス）を検知し、防御	◎		○	394,000円／月 *4
		URLフィルタリング					216,500円／月 *4
		ファイル検査 *1					280,500円／月 *4
	E-mailセキュリティ	ウイルス対策（E-mail）	スパムメールやメール添付型ウイルスといった脅威を解析・検知し、防御	◎		○	301,500円／月 *4
		スパムメール対策					301,500円／月 *4
		ファイル検査 *1					599,000円／月 *4
	アプリケーション/データベースセキュリティ	アプリケーションフィルタリング	お客さまポリシーに従って、アプリケーションを検出、通信を制御（アプリケーションプロファイリング含む）	◎		○	225,000円／月 *4
		WAF	Webアプリケーションに対する脅威（不正な通信およびウイルス）を検知し、防御				310,000円／月 *4
	PC/サーバーセキュリティ	ウイルス対策（PC/サーバー）	PC/サーバーにおいて、ウイルス感染を検知、防御	◎		○	基本料金315,000円／月 ＋ 600円/ID・月 *4
		仮想パッチ（脆弱性パッチ）	OS等の脆弱性に対する仮想パッチを自動適用し、既知の脅威からシステムを保護				基本料金315,000円／月 ＋ 12,500円/ID・月 *4
		VM間Firewall	VM間の通信（L4まで）を制御しシステムを保護				基本料金315,000円／月 ＋ 10,000円/ID・月 *4
情報漏洩対策	データセキュリティ	DLP *1	第3者（お客さまとサービス提供者以外）へのお客さま情報の漏洩を防止	◎		○	241,500円／月 *4
パッケージ	セキュリティエントリープラン		セキュリティ脅威から守る対象に対して、最も一般的かつ最低限のセキュリティ対策をパッケージ化	◎		○	208,000円／月 *4
	標的型攻撃対策プラン		標的型攻撃を代表とする未知の脅威、潜在リスクに対する入口・出口対策をパッケージ化	◎		○	346,500円／月 *4

*1（　　）：2012年9月28日の追加対象です。その他のメニューは2012年6月29日より提供開始しております。
*2:「運用レベル1」は監視検知および自動通知、「レベル2」は防御/脅威分析およびインシデントレスポンス、「レベル3」は改善提案（アドバイザリーレポート）です。◎は参考料金に含まれます。○は追加料金にて提供します。
*3: オンプレミス環境における参考料金です。料金はお客さまのシステム環境により異なります。　　*4: 月額料金です。別途、初期料金が必要です。

別紙　ネットワークプロファイリング

- お客さまネットワーク上にセキュリティ機器（アプリケーションファイアウォール）を設置し、セキュリティオペレーションセンタにてセキュリティ監視・運用・保守をします。
- 専門アナリストが、IDS/IPSのシグネチャーやウイルス対策のパターンファイルでは危険と判定されない通信も分析し、未知の脅威や潜在的なリスクを検出、可視化します。
- 分析結果をもとに危険度を判定し、対応方法をレポートします。



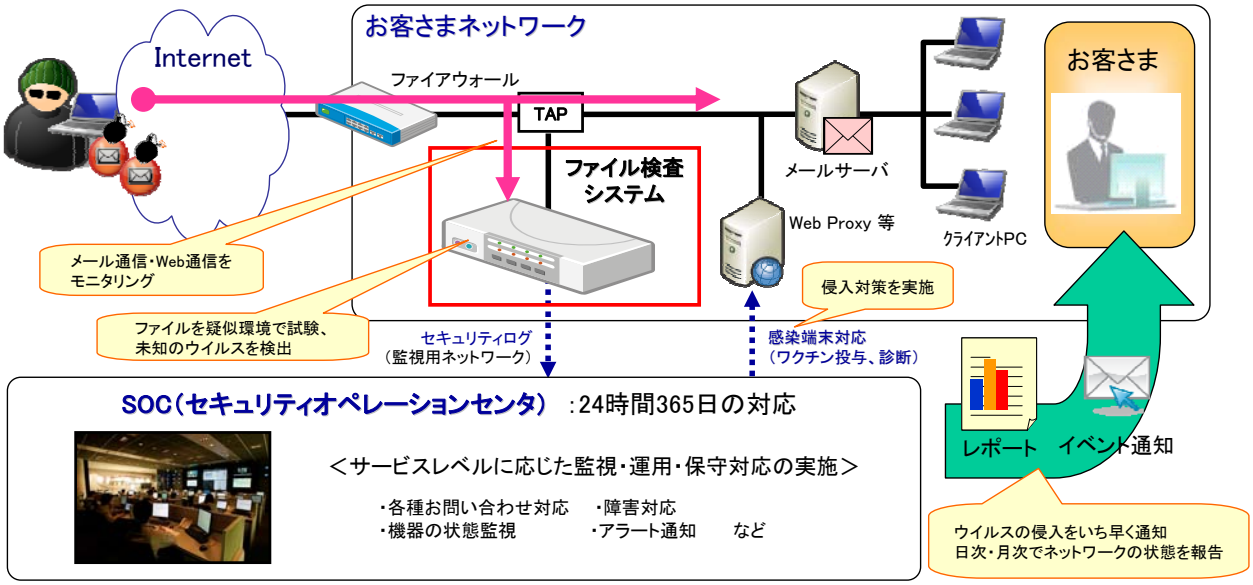
SOC（セキュリティオペレーションセンタ）　：24時間365日の対応

＜サービスレベルに応じた監視・運用・保守対応の実施＞

・各種お問い合わせ対応　・障害対応
・機器の状態監視　・アラート通知　など

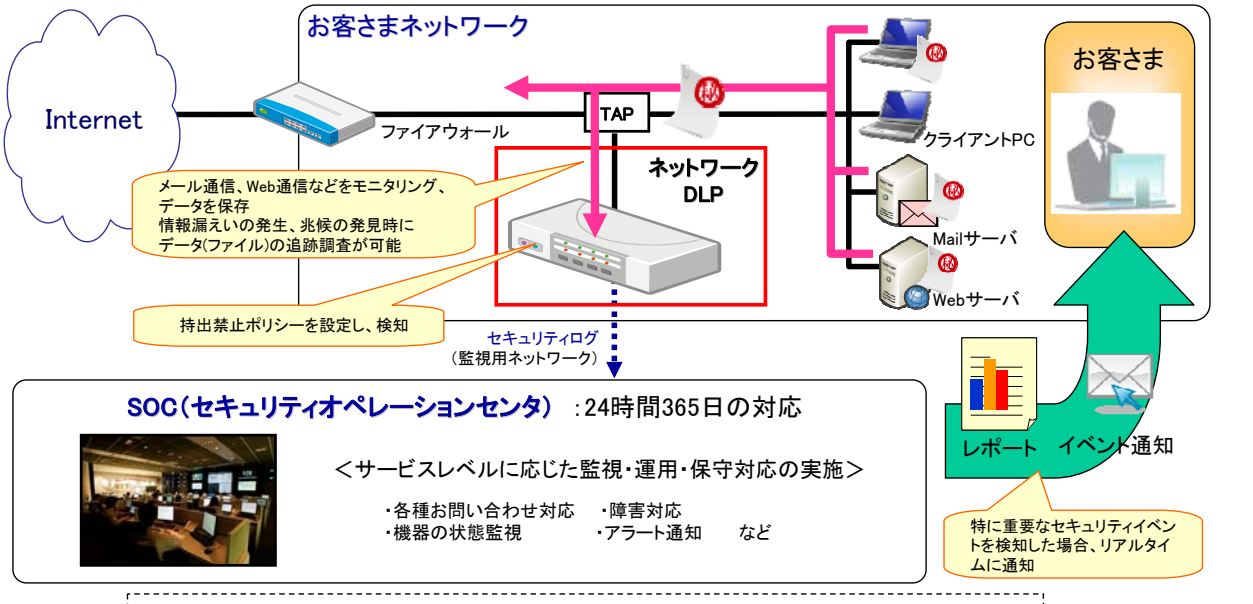
別紙 ファイル検査

- お客さまネットワーク上にセキュリティ機器（ファイル検査システム）を設置し、セキュリティオペレーションセンタにてセキュリティ監視・運用・保守をします。
- メールの添付ファイルやインターネットからのダウンロードファイルを隔離された安全な疑似環境で試験し、不審な動作をしないかを確認することで、他のウイルス対策では発見できないような未知のウイルスを検出できます。
- 他サービスと連携し、お客さまネットワークへの侵入対策も実施可能です。



別紙 DLP

- 情報の持出禁止ポリシーを設定したセキュリティ機器（ネットワークDLP）をお客さまネットワーク上に設置し、セキュリティオペレーションセンタにてセキュリティ監視・運用・保守をします。
- 外部との通信（メール通信、WEB通信など）を漏れなくモニタリングし、持出禁止ポリシーにマッチする送信ファイルを検出し、特に重要なセキュリティイベントはリアルタイムに通知します。
- お客さまの要望にあった持出禁止ポリシーの作成を支援します。



持出禁止ポリシー（例）

<ポリシー例①>
個人情報に関する以下のキーワードが
1ファイルの中に複数回含まれる場合に検知
・氏名 ・住所 ・メールアドレス ・クレジットカード番号のパターン

<ポリシー例②>
機密情報に関する以下のキーワードが
1ファイルの中に複数回含まれる場合に検知
・機密 ・非公開 ・厳秘 ・幹部会議資料