UNISYS

News Release

日本ユニシス株式会社　広報部
本社　〒135-8560 東京都江東区豊洲1-1-1

2021 年 5 月 20 日

日本ユニシス
事業継続の最重要課題「サイバーリスク対策」を実現する
マネージド・セキュリティー・サービス（MSS）を提供開始

～幅広い防御対象範囲をワンストップ対応、ニューノーマル時代のサイバーセキュリティー経営へ～

日本ユニシスは、クラウド活用や働き方改革が求められる企業向けに、サイバーセキュリティー経営を統合的に実現する「マネージド・セキュリティー・サービス（以下「MSS」）」を、本日から提供開始します。
MSS とは、経験豊富なセキュリティー専門家が、企業のサイバーセキュリティー体制やシステム、機器などの運用を代行し、有事の際の復旧支援をすることで、運用負荷とリスク低減を実現するアウトソーシングサービスです。
情報漏えいなどのサイバーリスク対策は、企業の事業継続にとっての最重要課題です。
日本ユニシスの MSS は、幅広い防御対象範囲を専任の担当者がワンストップで監視、対応支援します。また「ゼロトラスト・アーキテクチャー」の採用により、お客さまの IT 運用をさらに強力に支援し、ニューノーマル時代のサイバーセキュリティー経営を実現します。

【背景】
コロナ禍で拡大するテレワークや働き方改革の浸透により、企業のサイバーリスクは増大しています。特定非営利活動法人日本ネットワークセキュリティ協会（以下「JNSA」）「情報セキュリティーインシデントに関する調査報告書」(注 1) によると、個人情報の漏えい人数や件数は増加の一途をたどり、想定損害賠償総額は約 2,700 億円、1 件あたりの平均想定損害賠償額は約 6 億 4,000 万円となり、実際に被る損害の大きさがうかがえます。今やサイバーリスク対策は社会課題であり、企業の事業継続にとっての最重要課題です。

こうした中、日本ユニシスは新たな統合的 MSS の提供を開始します。専門知識を持った専任の担当者が、幅広い防御対象範囲をワンストップかつ網羅的に対応することで、サイバーリスクとともに有事の際の復旧負荷を低減します。さらに「ゼロトラスト・アーキテクチャー (注 2) 」を採用し、ニューノーマル時代のサイバーセキュリティー経営を実現します。

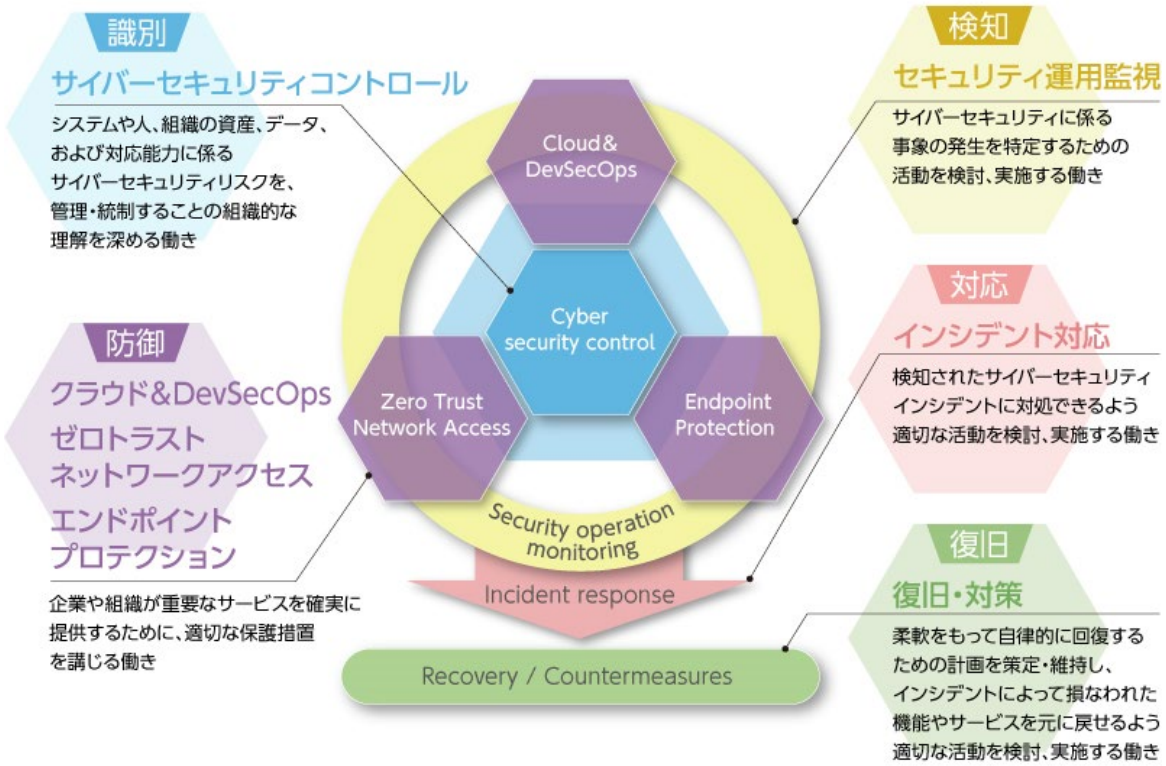
【マネージド・セキュリティー・サービス（MSS）の概要】
日本ユニシスの MSS は、経済産業省や独立行政法人情報処理推進機構（以下「IPA」）が策定した「サイバーセキュリティー経営ガイドライン Ver2.0」「実践のためのプラクティス集」に基づいており、サイバー攻撃による業務停止の迅速な復旧プロセスまで組み込んだビジネス上の実用性が高いサービスです。

「識別」「防御」「検知」「対応」「復旧」の 5 つのライフサイクル全般にわたり、サイバーセキュリティー経営への対策を管理、実行することで、経営者から CIO、CISO、IT/セキュリティー担当者を包括的に支援します。

1. サイバーセキュリティー経営の実践に必要不可欠な「基本サービス」です。継続的実施が求められるセキュリティー維持強化に役立ちます。
   - セキュリティーリスクや成熟度の可視化
   - セキュリティー診断
   - セキュリティー教育
   - CIO、CISO 戦略アドバイザリー（セキュリティー担当役員へのアドバイス）など
2. パブリッククラウド、ゼロトラスト、エンドポイントの 3 つの領域に重点をおき、各領域の対策を連動させた監視・運用が可能になります。（当社が対応）

3. サイバーセキュリティー対応の体制を整備し、緊急時での速やかな対応が可能になります。（当社が緊急対応を支援）

【マネージド・セキュリティー・サービス（MSS）の概要】



識別	セキュリティーリスクや成熟度の可視化、セキュリティー診断、セキュリティー教育、CISO 戦略アドバイザリー（セキュリティー担当役員へのアドバイス）など、サイバーセキュリティー経営の実践に必要不可欠かつ継続的実施が求められる「基本サービス」。
防御	「クラウド&DevSecOps」「ゼロトラストネットワークアクセス」「エンドポイントプロテクション」の領域を中心とした「防御と運用監視サービス」。 **①クラウド&DevSecOps** クラウド上のサーバー環境を保護するための対策と、運用監視サービス および DX 推進のための DevSecOps サービス。 市場ニーズや顧客要求に迅速に対応したり、自社の戦略を円滑に実行したい、といった例で自社の社員で開発したいと考える企業に、「シフト&レフト(※)」を実践し、セキュアなサービスを開発・運用できる DevSecOps の実践環境を提供します。 ※シフト&レフト：システムやサービスの開発において、より早い段階（より左側）で、セキュリティーを考慮した対応を行う。アジャイルや DevOps においては、継続的な開発・運用サイクルの中でセキュリティーの検査も継続的に、繰り返し行うことが重要である。
検知	**②ゼロトラストネットワークアクセス** ゼロトラストセキュリティー環境の構築および運用監視サービス。 「Verify and Never Trust」（決して信用せず常に確認）をコンセプトとする、「ゼロトラスト・アーキテクチャー（Zero Trust Architecture；ZTA）」に則った、データアクセス環境を提供します。 **③エンドポイントプロテクション** 高度な振る舞い検知型セキュリティーソリューションの導入および運用監視サービス。 セキュリティー侵害時の対応や、調査に重要な脅威の挙動を記録、監視しつつ、マルウェアの侵入や不正操作の防護を行います。テレワークで企業のセキュリティー領域外で利用されるノート PC などを、安全に利用できる監視運用のサービスを提供します。
対応	セキュリティーインシデントへの対応体制（CSIRT）の整備と緊急時のインシデント対応支援サービス。
復旧	インシデントの範囲や影響度、重要度に応じて、個別に対応方法を判断、提案します。

【今後の取り組み】

日本ユニシスの社内セキュリティー環境も、認証・デバイス管理・データ可視化・監視を含めた「ゼロトラスト・アーキテクチャー」を採用しています。サイバー攻撃の手法は日々新たなものが生まれ続けているため、当社内で得られた知見・経験を、お客さまにいち早く還元すべく、MSS の継続的な進化を進めてまいります。

以　上

注 1：JNSA「2018 年 情報セキュリティーインシデントに関する調査報告書」
https://www.jnsa.org/result/incident/2018.html

個人情報漏えいインシデント（概要データ）		
	2018 年	2017 年
漏えい人数	561 万 3,797 人	519 万 8,142 人
インシデント件数	443 件	386 件
想定損害賠償総額	2,684 億 5,743 万円	1,914 億 2,742 万円
1 件あたりの漏えい人数	1 万 3,334 人	1 万 4,894 人
1 件あたり平均想定損害賠償額	6 億 3,767 万円	5 億 4,850 万円
1 人あたり平均想定損害賠償額	2 万 9,768 円	2 万 3,601 円

注 2：ゼロトラスト・アーキテクチャー
組織の中と外との間に、ファイアウォールなどの機器で壁を作り、その中を安全と見なす今までの「境界型セキュリティー」では、ログイン ID やパスワードを第三者に奪われ、一度でも侵入を許してしまうと、その後の対策が難しくなります。この弱点を補い、全てのアクセスを信頼せず、常に利用者を認証し、監視の上でシステムの利用を許す、という構造をもっているのが「ゼロトラスト・アーキテクチャー」です。たとえ認証を突破されても、重要情報へのアクセスを制限したり、ネットワーク内での侵入者の行動を把握し、必要に応じて対処したりできます。

参考：IPA「情報セキュリティー10 大脅威 2021」
https://www.ipa.go.jp/security/vuln/10threats2021.html

2021 順位	組織への脅威	2020 年順位
1 位	ランサムウェアによる被害	5 位
2 位	標的型攻撃による機密情報の窃取	1 位
3 位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
4 位	サプライチェーンの弱点を悪用した攻撃	4 位
5 位	ビジネスメール詐欺による金銭被害	3 位
6 位	内部不正による情報漏えい	2 位
7 位	予期せぬ IT 基盤の障害に伴う業務停止	6 位
8 位	インターネット上のサービスへの不正ログイン	16 位
9 位	不注意による情報漏えい等の被害	7 位
10 位	脆弱性対策情報の公開に伴う悪用増加	14 位

参考：関連オンラインセミナー事前登録のお知らせ
2021 年 6 月 2 日（水）～4 日（金）BITS2021 内 P-10
「DX 時代に向けたセキュリティーアーキテクチャー」
https://bits.unisys.co.jp/2021/tokyo/program.html

■関連リンク：
「マネージド・セキュリティー・サービス（MSS）」
https://www.unisys.co.jp/solution/tec/security/lp/
情報セキュリティーサービス「iSECURE」
https://www.unisys.co.jp/solution/tec/security/
経済産業省「サイバーセキュリティー経営ガイドライン Ver 2.0」
https://www.meti.go.jp/policy/netsecurity/mng_guide.html
IPA「サイバーセキュリティー経営ガイドライン Ver 2.0 実践のためのプラクティス集」
https://www.ipa.go.jp/security/fy30/reports/ciso/index.html

※iSECURE は、日本ユニシスの登録商標です。
※その他記載の会社名および商品名は、各社の商標または登録商標です。
※掲載の情報は、発表日現在のものです。その後予告なしに変更される場合がありますので、あらかじめご了承ください。

<本ニュースリリースに関するお問い合わせ>
https://www.unisys.co.jp/newsrelease_contact/