DX時代の企業競争で求められる エンドポイントセキュリティ

IDC
ANALYZE THE FUTURE

An IDC InfoBrief, Sponsored by イーセットジャパン | November 2019

新たな技術を活用したデジタルトランスフォーメーション(DX)の取り組みによって企業の競争力が高まる

DXへの取り組みは、クラウドやモバイル、ビッグデータ解析、ソーシャル技術などの新たな技術を活用することで新規ビジネスを創出し、リアルタイムな顧客サービスによって顧客満足度の向上を実現し、その結果として、企業競争力が高まる

Phase 1
新たな技術を活用する

Phase 2
変革を起こす

リーダーシップ変革
変革を起こすためのリーダーシップ

オムニエクスペリエンス変革
サプライヤーと顧客のリアルタイムなコミュニケーションによって顧客満足度を高める

情報変革
データ活用を促進させることで、データの価値が高まる

運用モデル変革
開発から運用までの迅速化と運用の自動化を図る

ワークソース変革
働き方改革を進める

Phase 3
変革を拡大させる

リーダーシップの拡大
継続的に変革を起こすためのリーダーシップの促進

共感の拡大
サプライヤーと顧客のリアルタイムなコミュニケーションによって共感をさらに高める

洞察の拡大
AIなどのデータ分析によって目的に合ったデータを作成し、データ活用を促進させ、利用範囲を拡大させる

自己回復力の拡大
運用の自動化によって自己回復力を高める

ワークモデルの拡大
働き方改革を促進させ、継続する

IDC
ANALYZE THE FUTURE

DXを成功させるためには変革を拡大していくことが重要

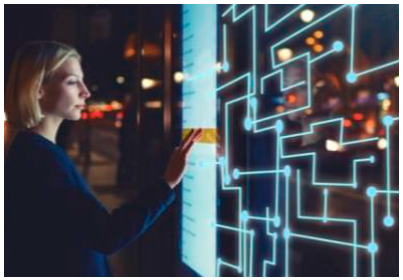
DXの進展を加速させるためには、「インテリジェントコア」を中核としたDXプラットフォームの構築が必要

文化の未来 リーダーシップの拡大

KPI（主要業績評価指標）やMBO（目標管理制度）などを活用し、変革する文化を浸透させる。

顧客の未来 共感の拡大

顧客との共感を従業員、パートナー、サプライヤー全員にとって最重要目標と位置付けて、業務やプロセス、技術を変革していく。



インテリジェンスの未来 洞察力の拡大

AIや機械学習によるデータの活用によって、全社レベルで製品およびサービス価値を向上させる。

オペレーションの未来 自己回復力の拡大

分散し拡大する業務システムを共通のプラットフォームに統合し、複雑なプロセスの自動化や迅速な意思決定を可能にする運用へと変革させる。

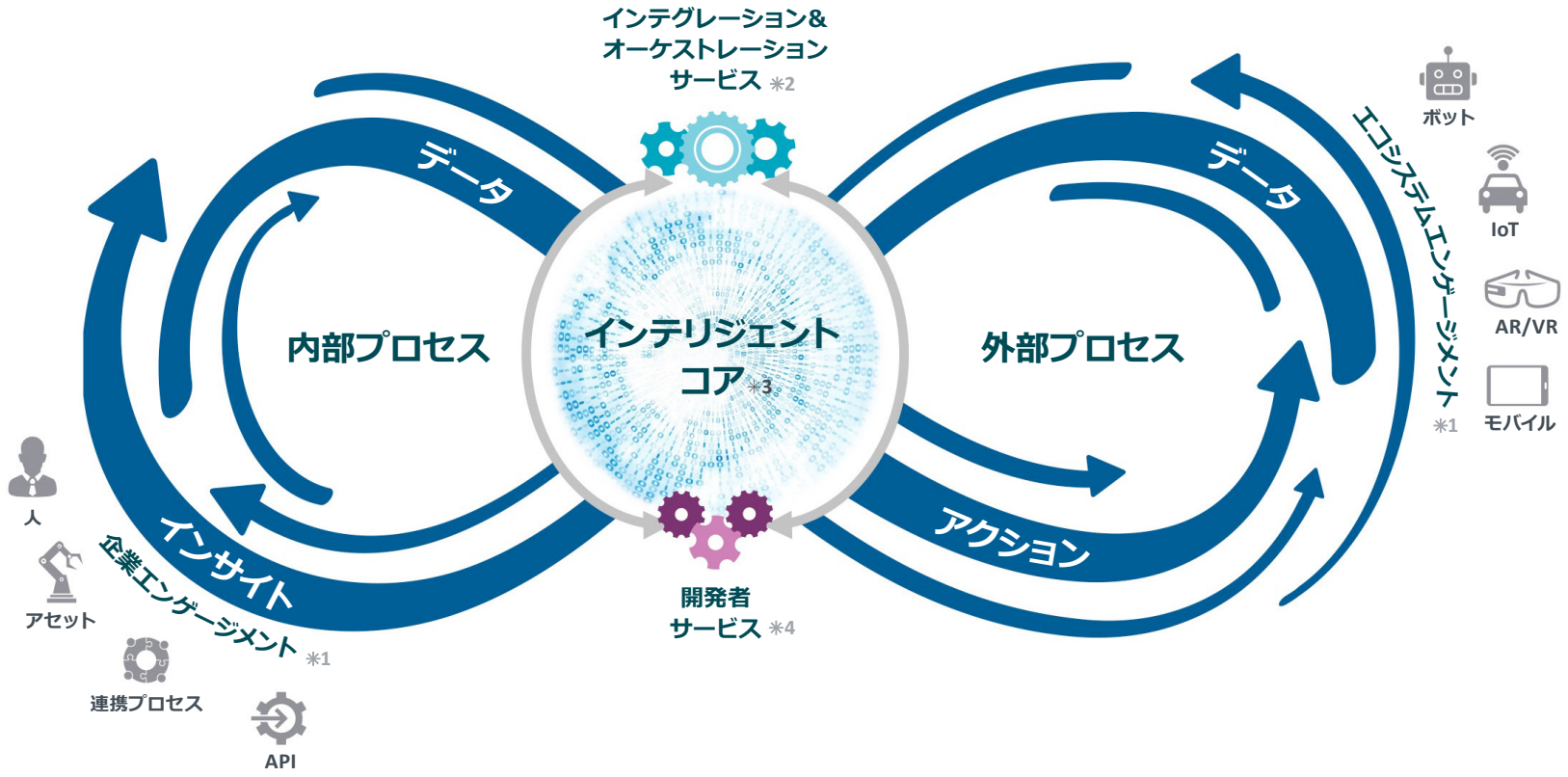
働き方の未来 ワークモデルの拡大

デジタル技術で多様化する働き方について、企業全体で一貫した働き方変革を進める。

DXプラットフォームにより、ビジネスの拡大を促進、企業のDXを加速

DXプラットフォーム

データ活用を促進させる「インテリジェントコア」を中核としたプラットフォームであり、「インテリジェントコア」によってデータを循環させ、データ活用を拡大させる



✳1: **企業／エコシステムエンゲージメント**:デザイン思考に基づいたインタラクションによってユーザー体験を向上し、外部および企業内のエコシステムを活性化するサービス

✳2:**インテグレーション&オーケストレーションサービス**:組織や機能ごとに分散化した「サービス(プロセス／データ)」をAPIを介して連携、統合、構成し、デジタルビジネスの実現を支援する運用／管理サービス

✳3:**インテリジェントコア**:DXプラットフォームの中核として、多様なデータを収集、分析し、改善、改革するためのアクションを導き出す「データサービス」プラットフォーム

✳4:**開発者サービス**:クラウドネイティブアプリケーションの開発および実行環境を提供

IDC
ANALYZE THE FUTURE

DXを進展させることでセキュリティリスクが拡大

特にDXプラットフォームによってセキュリティリスクが拡大し、複雑化する

文化の未来 リーダーシップの拡大

KPI（主要業績評価指標）やMBO（目標管理制度）などを活用し、変革する文化を浸透させる。

顧客の未来 共感の拡大

サプライチェーンリスクとモバイル／クラウドへのリスク

顧客やパートナー、サプライチェーンとの共感を拡大することで、サプライチェーンリスクおよびコミュニケーション環境であるモバイル環境とクラウド環境でのセキュリティリスクが高まる。

インテリジェンスの未来 洞察力の拡大

データ侵害と信頼性へのリスク

インテリジェント化したデータ活用の拡大で、データ侵害と信頼性へのリスクが高まる。

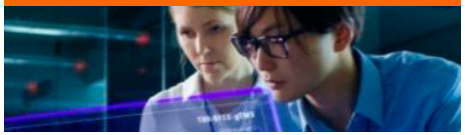
オペレーションの未来 自己回復力の拡大

開発／運用での脆弱性リスク

運用の自動化が進むことで、システム開発とシステム運用における脆弱性リスクが高まる。

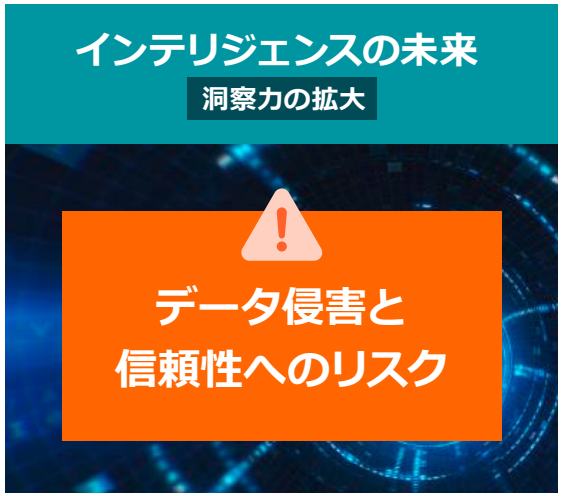
働き方の未来 ワークモデルの拡大

シャドーITリスク

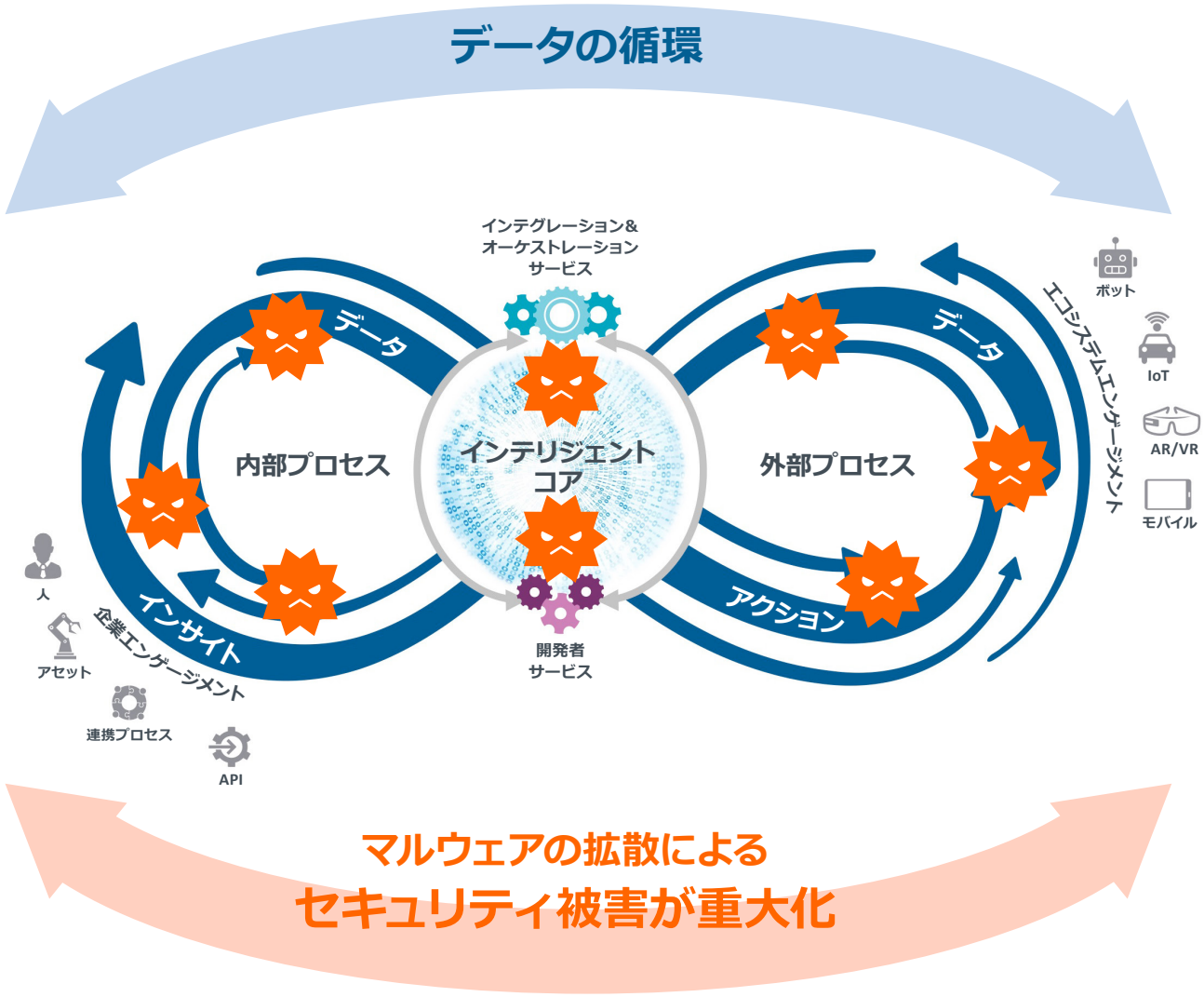


働き方変革によって、場所や時間に関わらず情報資産の活用が行われるため、許可していないIT資産（シャドーIT）における情報漏洩リスクが高まる。

DX進展の加速によってデータ活用が拡大、セキュリティ被害が重大化

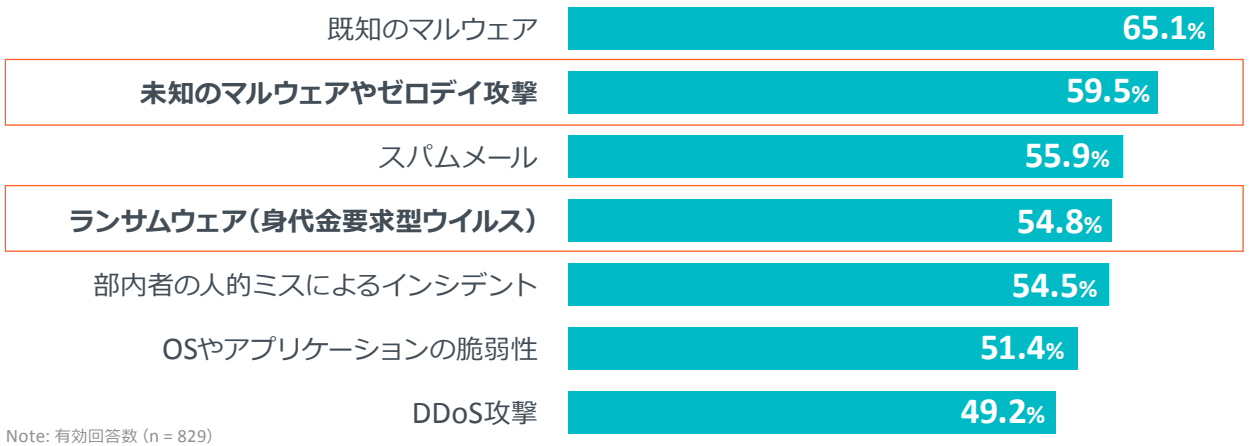


- データ活用を拡大していくには、信頼性のあるデータを循環させることが必要である。
- だがDX環境では、一部のシステムがマルウェアに感染した途端に、マルウェアは拡散され、セキュリティ被害が重大化する。
- そのため、データ侵害を防ぐと共に、侵害が発生しても早期に検知し対処できるセキュリティ体制が求められる。



サイバー攻撃の高度化によって高まる高度なマルウェアへの懸念

懸念されるセキュリティ脅威



Note: 有効回答数 (n = 829)

未知のマルウェアやランサムウェアといった高度なマルウェアへの懸念が上位にリストアップされている

従来のウイルス対策製品で高度なマルウェアを防御できるか？

Q 未知のマルウェアやゼロデイ攻撃は従来のウイルス対策製品で防御できますか？

A 従来のウイルス対策製品は、検出したマルウェア検体からシグネチャを作成し、そのシグネチャと照合して合致したものを隔離して駆除します。しかし、未知のマルウェアやゼロデイ攻撃では、検体の入手が困難であるため、従来のウイルス対策製品ではシグネチャによる検出はできず、ウイルス感染を引き起こす恐れがあります。

Q ランサムウェアは従来のウイルス対策製品で防御できますか？

A 高度なランサムウェアは、自身のソースコードに少し手を加えてシグネチャを変更するなどして、ウイルス対策製品からの検出を回避するものもあり、従来のウイルス対策製品では防御することはできません。

IDC ANALYZE THE FUTURE

高度化するサイバー攻撃でサイバーセキュリティ規制の強化が国際的に波及、国内企業へも影響

一般データ保護規則（EU GDPR）

72時間以内報告義務リスク管理とインシデント対応の義務

ネットワークおよび情報セキュリティ指令（NIS指令）

重要インフラ事業者およびサービスプロバイダーが対象で、報告義務とリスク管理、インシデント対応の義務がある

プライバシーシールド

カリフォルニア州消費者プライバシー法（CCPA）

データ侵害通知法

FedRAMP

政府が調達するクラウドサービス事業者のNISTに基づいた認証プログラム

NIST CSF

侵入を前提としたフレームワーク

NIST SP800-53

NIST SP800-171

政府調達に参加する企業およびサプライチェーン全体におけるCUI保護規則

欧米のサイバーセキュリティ規制は国内企業に影響を与えるか？

Q 国内企業には影響がないですか？

A EU GDPRは、EUの住民の「個人データ」が含まれている場合は、EU圏外の地域であってもEU GDPRが適用されます。
また米国政府調達における管理すべき重要情報（CUI）の保護に対する政府以外の企業や組織に適用されるセキュリティ対策基準「NIST SP800-171」は、サプライチェーンに対する適用も求められているため、米国政府調達関連企業と取り引きのある日本企業においても基準に沿った対応が求められ、日本企業も影響を受けます。これらの規制によって、プライバシーデータを含む重要データの保護と、侵入を前提としたレジリエンス（回復力）の強化が求められます。

サイバー攻撃に対するレジリエンス（回復力）を強化しないとビジネス競争から取り残されてしまう

日本においてもデジタル化の促進と共に、サイバーセキュリティに対する規制強化が進む

サイバーセキュリティに関わる現時点の国内法およびガイドライン

サイバーセキュリティ基本法

重要インフラ事業者はサイバーセキュリティに関する取り組みへの自主努力が求められる。

改正個人情報保護法

2017年5月30日に全面施行され、すべての企業と組織に適用されることになった。欧米のプライバシー法と比べ、改正個人情報保護法では情報漏洩の報告義務が課せられていない。

サイバーセキュリティ経営ガイドライン

セキュリティ対策は経営者が関与すべき事案であり、侵入を前提に侵害を最小限に抑えることを求めている。

デジタル行政に向けた今後の取り組み

行政手続きのデジタル化の促進

2019年5月に行政手続きを原則として電子申請に統一する「デジタルファースト法」が成立し、2019年度から順次実施される。

政府のクラウド活用の促進

政府は、クラウドサービスの利用を第一とする「クラウド・バイ・デフォルトの原則」を採用し、中央官庁および地方自治体でのクラウド活用を促進させていく。

セキュリティ規制強化に向けた今後の検討事項

改正個人情報保護法の見直し

現行の改正個人情報保護法の見直しが2020年に予定されている。この見直しで報告の義務化と削除権などが検討されている。

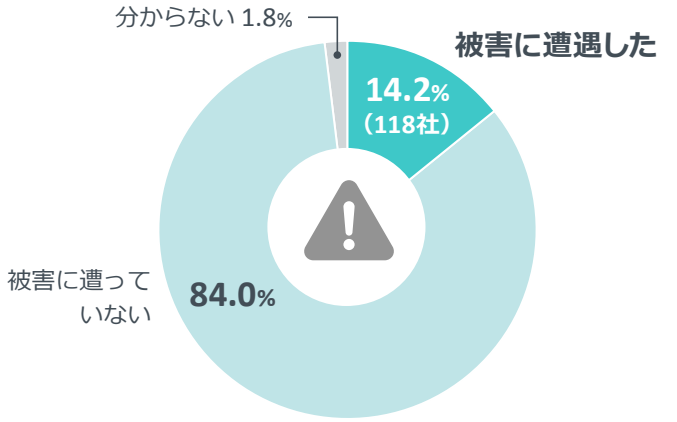
クラウドサービスの安全性評価制度（日本版FedRAMP）

クラウドサービスの利用を促進するために、サイバーセキュリティに対する安全性を評価し信頼できるクラウドサービスを選定する評価制度プログラムであり、中央官庁および地方自治体に提供するクラウドサービス事業者はこの評価制度で認証を受けることが求められる。制度の運用開始は2020年秋の予定となっている。

高度化するサイバー攻撃に対して、現状の対策では不十分

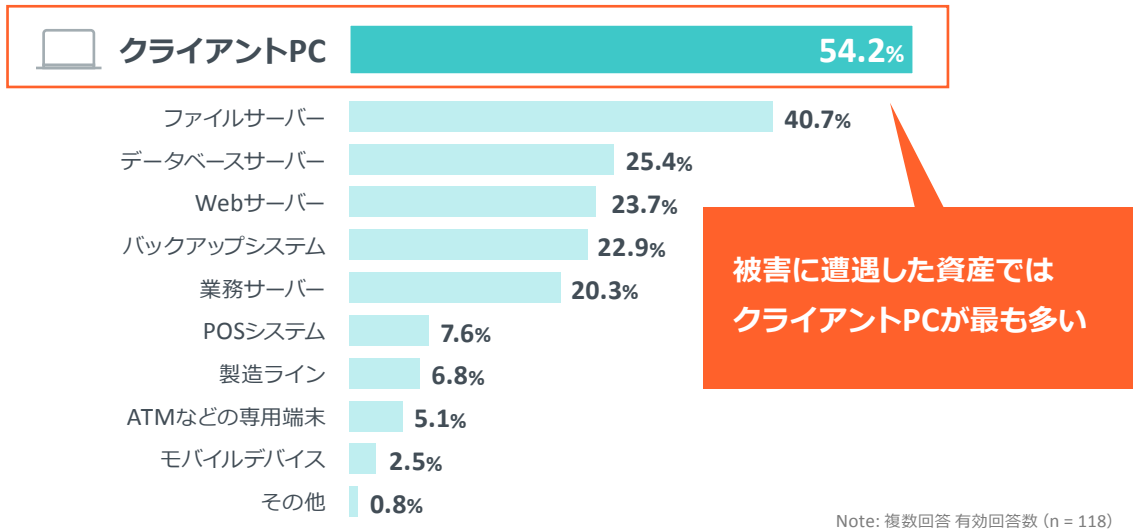
クライアントPCでのセキュリティ被害が最も多く、
セキュリティシステムによって攻撃を完全に防御することは困難な状況になっている

この1年間で被害に遭った企業



Note: 有効回答数 (n = 829)

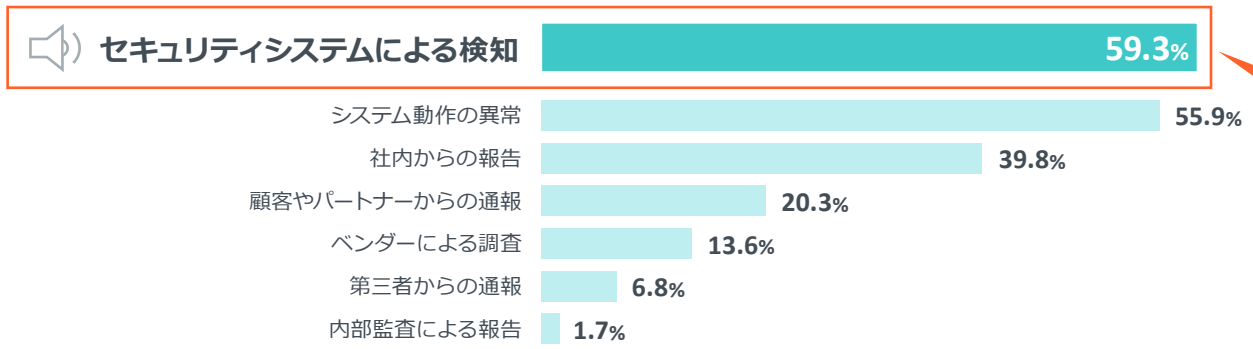
被害に遭った資産



被害に遭遇した資産では
クライアントPCが最も多い

Note: 複数回答 有効回答数 (n = 118)

被害の発見方法



セキュリティシステムによる
検知での発見は6割に留まり、
完全に防御できる状況でない

Note: 複数回答 有効回答数 (n = 118)

IDC
ANALYZE THE FUTURE

侵入前提のリスクアプローチによるサイバーセキュリティ

「完全な防御は不可能」との前提に立ち、
侵入されても早期に異常を検知し対処できる総合エンドポイントセキュリティソリューションの導入が必要

防御

サイバーレジリエンスの強化

セキュリティ侵害を前提にシステム破壊など不測の事態
が発生しても、早期に復旧できる体制の構築が必要

検知

脅威ライフサイクル

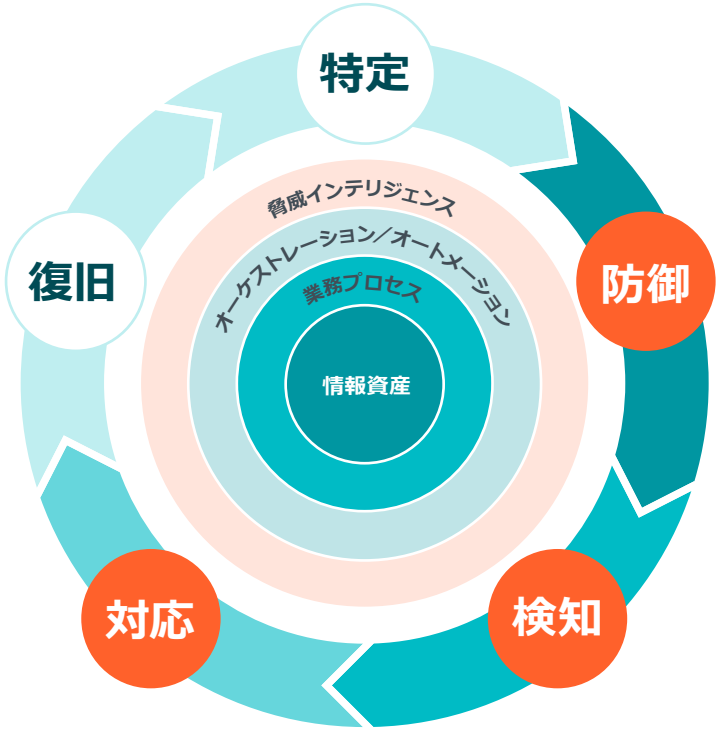
セキュリティ侵害を前提として、「特定」「防御」「検知」
「対応」「復旧」の5つのフェーズで対策を実施

対応

高度なマルウエアへの対応

侵入を試みるマルウェアからの防御と、
侵入したマルウェアの早期検知および対応

脅威ライフサイクル

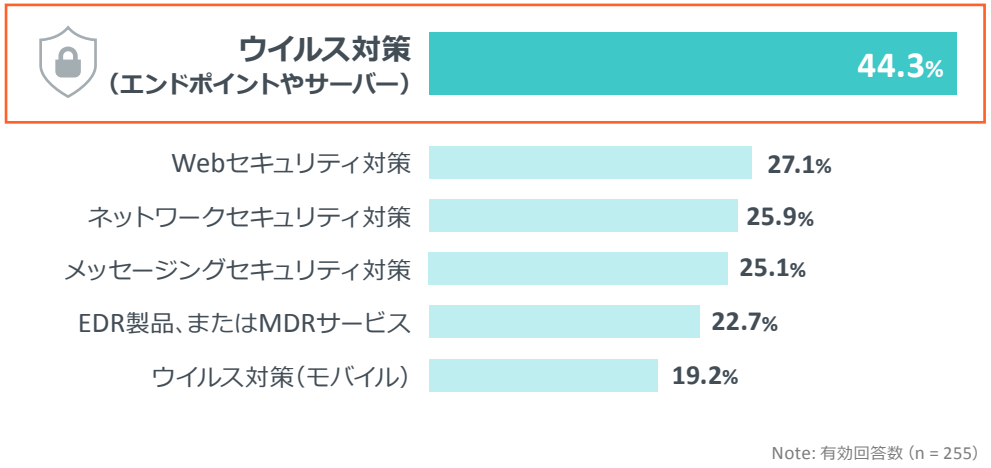


IDC
ANALYZE THE FUTURE

投資はエンドポイントセキュリティに偏在
セキュリティソリューション導入の最大の課題は予算

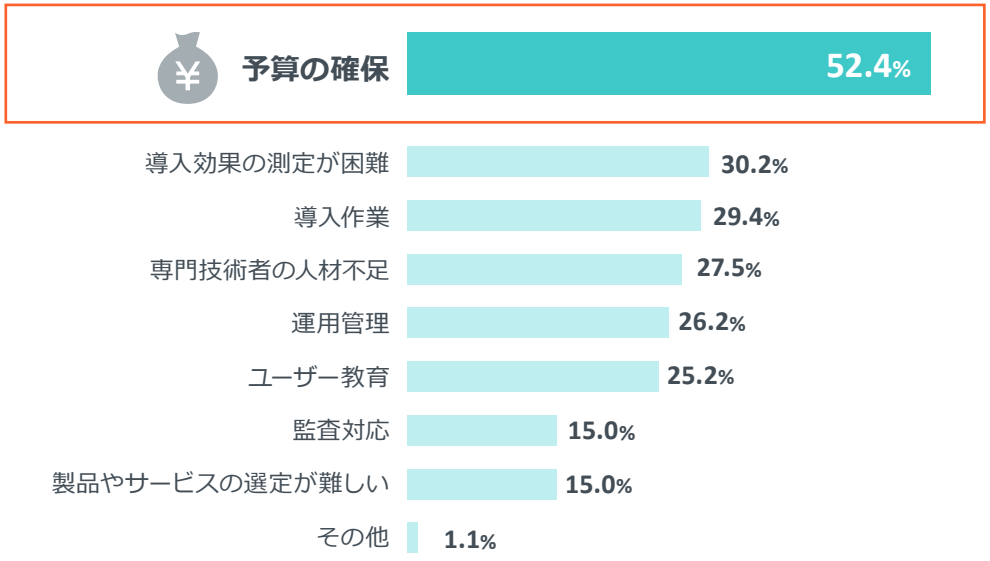
- ☑ エンドポイントセキュリティへの投資優先度が高い
- ☑ 最大の課題は予算である。次いで、導入効果、導入作業、人材不足、運用管理が続く

2019年のセキュリティ投資を増やす企業の外部脅威対策投資重点項目



Note: 有効回答数（n = 255）

セキュリティ導入の際の課題



Note: 有効回答数（n = 829）

高度化するサイバー攻撃に対して総合エンドポイントセキュリティソリューションが必要

DXによって起こる先進技術の採用によるリスク

- DXの進展によるセキュリティリスクの拡大と被害の重大化
- 高度化するサイバー攻撃による攻撃対象の拡大とセキュリティ対策の複雑化
- 不安定要素のある先進技術を採用した環境で完全な防御は困難

DXを進めるユーザー企業の課題

- 予算が最大の課題である
- 導入効果の測定が難しい
- 人材不足と製品の複雑化によって導入／運用管理が難しい

課題解決

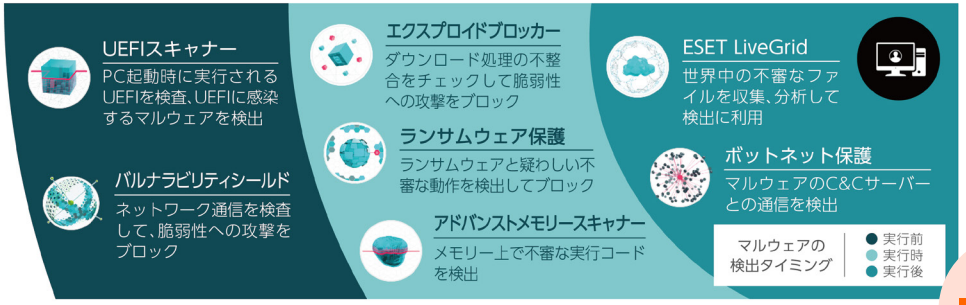
ユーザーが求めるエンドポイントセキュリティ

- コストパフォーマンスが高いこと
- 導入／運用が容易であること
- 防御から検知／対応まで行える総合的なソリューションであること

イーセットが提供する
エンドポイントセキュリティとは

使いやすさ、対応スピード、コストについて妥協することなく最高レベルの保護を実現

多層防御アプローチでエンドポイントのすべての層において高度な防御機能を提供



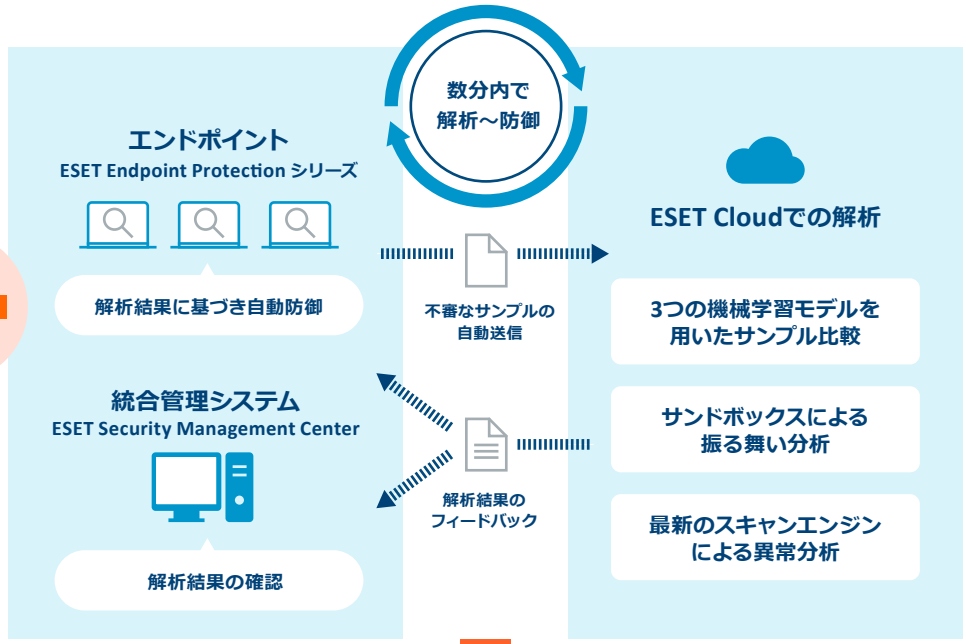
お客様、独立系テスト機関などからの高い評価

高い検知率	誤検知の低さ	軽快さ	導入・運用性

- エンドポイントソフトウェア 導入実績 39万1,000社
- エンドポイントセキュリティソフトウェア市場 中堅中小企業で国内シェア第3位*

*Source: IDC Japan Semiannual Security Software Tracker, 2018H2 Final Historical & Forecast （2019年7月）

さらにクラウド解析を駆使した新たな防御層を追加



- 巧妙なマルウェアも確実に防御

Source：イーセットジャパン, November 2019

高度化するサイバー攻撃に対して
総合エンドポイントセキュリティが必要

✔ トータルエンドポイントソリューション

EDR の導入によって侵入されても早期に検知・対処できるソリューションを提供。さらに脅威の予測にも対応。

✔ 『使える』『選べる』ソリューション:

製品性能だけでなく、
運用・導入のしやすとコストパフォーマンスを同時に実現。

✔ 安 心

キヤノンマーケティングジャパンによるサポート。

✔ 継続的な技術開発

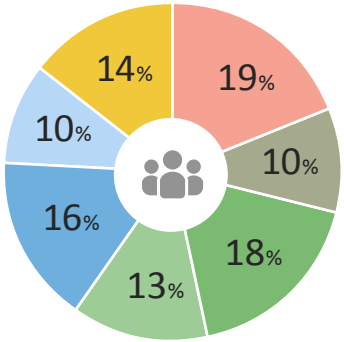
株価に左右さないプライベートカンパニーのため長期的な視野に立った経営により、エンドポイントセキュリティ技術への開発投資を継続。

Source：イーセットジャパン, November 2019

調査方法

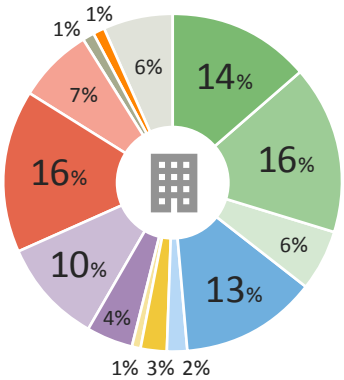
本調査レポートは、IDC Japanが2019年4月に実施した情報セキュリティ対策の導入実態調査の結果を基に作成した。アンケートでは、国内企業（官公庁も含む）の情報セキュリティ対策の導入実態と今後の方向性などを調査した。

回答者属性 **従業員規模別**



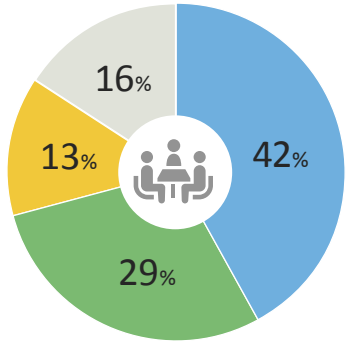
- 10人未満
- 10～99人
- 100～249人
- 250～499人
- 500～999人
- 1,000～2,999人
- 3,000人以上

回答者属性 **業種別**



- 金融
- 製造
- 建設／土木
- 小売／卸売
- 交通／運輸
- 通信／メディア
- 公益（エネルギー関連）
- 福祉／医療
- 教育
- 情報サービス
- その他サービス
- 中央官庁および外郭団体
- 地方自治体関連
- その他

回答者属性 **セキュリティ導入に対する立場**



- 情報セキュリティの導入に関する決定権がある
- 情報セキュリティの導入を検討する立場である
- 情報セキュリティの導入に関して、アドバイスや意見を行う
- 情報セキュリティの導入状況を知っている

Note: 有効回答数（n = 829）