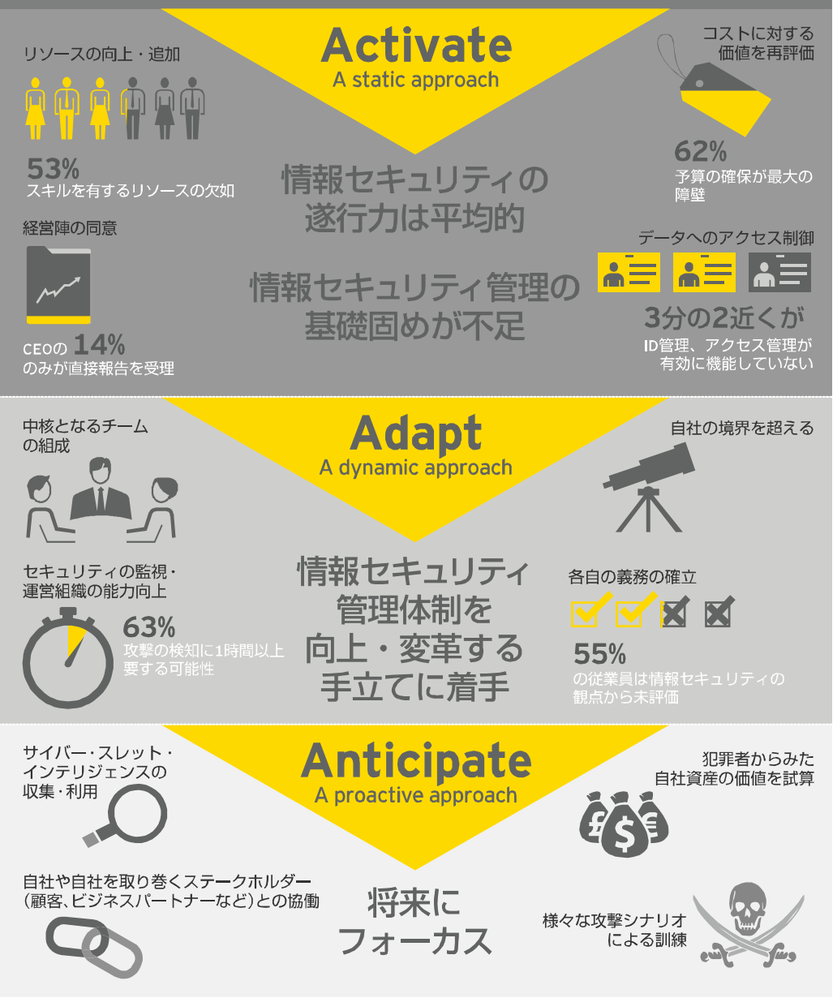
EY2014 グローバル情報セキュリティサーベイ主要調査結果

56% の組織が手口の巧妙なサイバー攻撃を検知することができない

サイバー犯罪に先手を打つためには？



グローバル情報セキュリティサーベイ（GISS）は、今回で17年目を迎えます。この種の調査では最も長期にわたって実施されており、その調査結果はクライアントが自社の情報セキュリティの課題を他社と比較することによって、重要な意思決定するための有用な情報としてお役立て頂いております。

グローバル全体にかかわる報告書および詳細な解説については、弊法人担当もしくは下記のお問合わせ先までご連絡ください。

サイバー犯罪に先手を打つ
EYによる2014年
グローバル情報セキュリティサーベイ

（英文版）
www.ey.com/giss
（日本語版）
www.shinnihon.or.jp/tl/giss

EYではビジネスリスクやシステムリスクに関連した課題などに焦点をあてた刊行物「Insights on governance, risk and compliance」を発行しています。

「Insights on governance, risk and compliance」の日本語版については、新日本有限責任監査法人のホームページ
http://www.shinnihon.or.jp/services/advisory/risk-advisory/global-contents/index.html をご覧ください。
英文版については、www.ey.com/GRCinsights をご覧ください。

お問合わせ先

新日本有限責任監査法人 アドバイザリー事業部
東京都千代田区霞ヶ関3-2-5
霞ヶ関ビルディング28F
Tel：03 3503 3500
Fax：03 3503 1966
E-Mail:　AS-Markets@shinnihon.or.jp

EY | Assurance | Tax | Transactions | Advisory

EYについて
EYは、アシュアランス、税務、トランザクションおよびアドバイザリーなどの分野における世界的なリーダーです。私たちの深い洞察と高品質なサービスは、世界中の資本市場や経済活動に信頼をもたらします。私たちはさまざまなステークホルダーの期待に応えるチームを率いるリーダーを生み出していきます。そうすることで、構成員、クライアント、そして地域社会のために、より良い社会の構築に貢献します。

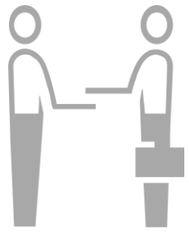
EYとは、アーンスト・アンド・ヤング・グローバル・リミテッドのグローバルネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。詳しくは、ey.comをご覧
ください。

新日本有限責任監査法人について
新日本有限責任監査法人は、EYメンバーファームです。全国に拠点を持つ日本最大級の監査法人業界のリーダーです。監査および保証業務をはじめ、各種財務アドバイザリーの分野で高品質なサービスを提供しています。EYグローバルネットワークを通じ、日本を取り巻く経済活動の基盤に信頼をもたらし、より良い社会の構築に貢献します。詳しくは、www.shinnihon.or.jp をご覧ください。

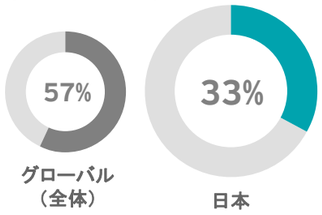
ED None

内部からの脅威に対して楽観的な日本企業

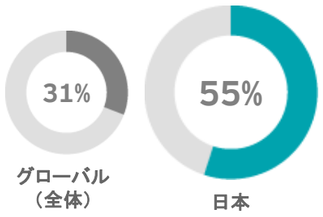
- グローバル（全体）では従業員や常駐する契約社員など組織内部の脅威（サイバー攻撃）を大きく意識していることに対し、日本では依然として犯罪組織やハッカーなど外部からの攻撃を脅威と感じているという結果になりました。



従業員 を潜在的な脅威主体とみなしている。



- 同様に、インサイダーリスクといった内部脅威に関連する情報セキュリティ投資の優先度も日本は低いという結果となり、危機感だけでなく、具体的施策の実施についても積極的ではない様子がうかがえます。



インサイダーリスクへの投資の優先度が 低い。

- 一方で、リスクにさらされる確率に最も大きな影響を及ぼした直近の脅威や脆弱性に関する質問では、回答傾向が投資優先度とは異なる一方、グローバル（全体）の傾向との一致がみられ、従業員の不注意や無自覚、不適切なデータ保管といった内容が上位となりました。

リスクにさらされる確率に最も大きな影響を及ぼした直近の脅威・脆弱性トップ5

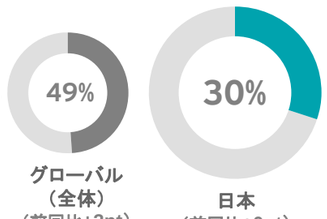
	日本	グローバル
1位	従業員の不注意もしくは無自覚	従業員の不注意もしくは無自覚
2位	マルウェア（ウイルス、ワーム、トロイの木馬など）	マルウェア（ウイルス、ワーム、トロイの木馬など）
3位	期限切れの情報セキュリティコントロールまたはアーキテクチャ	フィッシング詐欺
4位	モバイルコンピューティングの利用に関する脆弱性	期限切れの情報セキュリティコントロールまたはアーキテクチャ
5位	不正アクセス（不適切なデータ保管場所など）	クラウドコンピューティングの利用に関する問題

- 2014年に日本で発生した情報流出にかかるインシデントを踏まえると、組織内部から行われる不正アクセスに対する関心が高まっていることが予想され、脅威認識は今後変化する可能性があります。

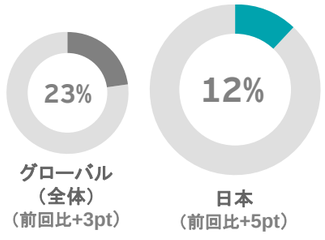
情報セキュリティ対策への戦略的アプローチが課題

- グローバル（全体）では49%、日本では30%の企業が情報セキュリティ戦略とビジネス戦略が整合していると回答しました。前回調査と比較すると、日本の結果が横ばいである一方、グローバル(全体）では3ポイントの増加となりました。

ビジネス戦略と整合した情報セキュリティ戦略を策定している。



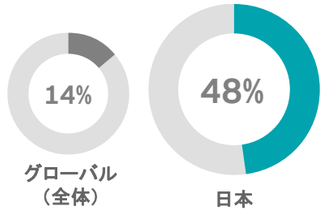
- また、情報セキュリティ戦略において、3年から5年の中長期計画を盛り込んでいる企業の割合は、日本では12%にとどまりました。
ただし前回の調査と比較すると、グローバル（全体）、日本共に上昇傾向にあり、3～5ポイント増加しています。



情報セキュリティ戦略に
中長期計画
を盛り込んでいる。

- さらに日本では、情報セキュリティ管理を行う上で、セキュリティ基準やフレームワークを利用していないと回答した割合が48%にのぼりました。

情報セキュリティ管理にセキュリティ基準やフレームワークを
利用していない。



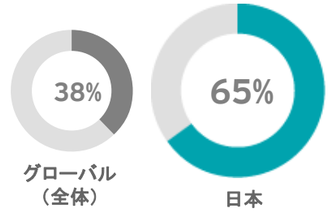
- 情報セキュリティ戦略の策定に関して、日本では、全体像の把握や施策領域の特定、組織内の意思疎通や戦略の進捗把握の基盤となるフレームワークの導入が喫緊の課題となっている状況がうかがえます。

情報セキュリティ管理に利用する基準・フレームワークトップ3

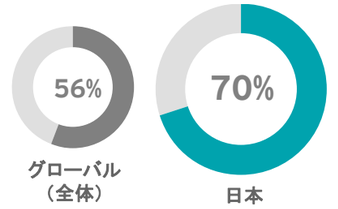
	基準・フレームワーク名	日本	グローバル
1位	ISO/IEC 27001 (ISMS)	25%	50%
2位	ITIL	16%	49%
3位	COBIT	14%	40%

インシデント対応体制構築は発展途上

重大なインシデントは最近
発生していない。



- 日本ではごく最近重大なインシデントは発生していないとの回答が65%と半数を上回りました。その一方、70%の企業が標的型攻撃などの巧妙化する攻撃を自組織が検知できる可能性は低い、またはかなり低いと回答しています。

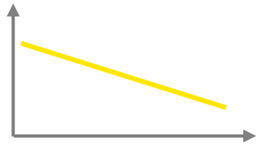


巧妙な攻撃を
検知できる可能性は 低い。

この結果は、実際にはインシデントが発生しているものの、検知できていない可能性を示唆しています。

情報セキュリティ投資の傾向は変わらず

- 情報セキュリティ費用に占める運用・保守費用の割合は、日本では、過去12ヶ月の平均は62%でしたが、今後12ヶ月の平均では57%に下がるという結果となりました。グローバルでも、過去12カ月の平均が53%、今後12カ月の平均は50%となり、同様に低下傾向が見られます。



情報セキュリティ費用における
運用・保守費用の割合は
3期連続低下傾向が見られる。

その一方、向上・拡充といった新しい取り組みへの予算配分が増える傾向が見られ、特に日本においては前回の調査から明らかな増加がみられます。