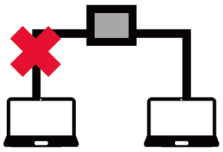
D1 CISOへ報告 2h

「PC1の利用者が不審なメールの添付ファイルを開封してしまったこと」をCISOへ報告します。

D2 セキュリティ情報を収集 1h

インターネットから、同様の不審メール発生状況や対策方法等の情報を収集します。

D3 PC1をネットワークから隔離 1h



PC1をネットワークから隔離します。

D4 開封した不審メールを調査 2h

開封した不審メールの調査をセキュリティベンダへ依頼します。

D5 Eラーニングを実施 3h

不審メール受信時に適切に対応できるよう、Eラーニングを実施します。

D6 メールセキュリティ製品を導入 4h

メールセキュリティ製品を導入し、従業員のメールボックスに届く不審メールを低減します。

D7 PC1の利用者へヒアリング 1h

メール開封時の操作やその後、端末の挙動に変化がないか等をヒアリングします。

D8 他従業員の不審メール受信状況を確認 2h

同様の不審メールを受信した従業員が他にいないか、情報システム部門に確認を依頼します。

D9 全従業員へ注意喚起 2h

当社を狙った不審メールが発生しているため、開封しないよう注意喚起します。

D3 PC1をネットワークから隔離 100 pt

他端末へのマルウェア感染拡大を防ぐことができました。

マルウェア感染拡大防止のため、感染の疑いのある端末はマルウェアを完全に駆除するまでネットワークから隔離（LANケーブル抜線・Wi-Fiオフ等）することが必要です。

D2 セキュリティ情報を収集 60 pt

同様の不審メールに関する情報は見つかりませんでした。

JPCERT/CCやIPAのホームページでは、最新のセキュリティ脅威情報や対策方法を公開しています。

日頃から最新情報をチェックしましょう。

D1 CISOへ報告 20 pt

CISOから、影響について詳細説明を求められました。

CISOへの報告は、インシデントの重大性に応じて内容やタイミングを考慮しましょう。

日常的に発生する軽微なセキュリティ事故（重大事故へ発展しないもの）であれば、まとめて月次などの報告とすれば十分です。

あらかじめ、報告基準を定めておくことが重要です。

D6 メールセキュリティ製品の導入 0 pt

セキュリティベンダより「メールセキュリティ製品の導入には１ヶ月必要」と連絡がありました。

メールセキュリティ製品の導入は、不審メールへの有効な対策ですが、導入には時間がかかります。

計画的に導入を進めましょう。

D5 Eラーニングを実施 20 pt

全従業員が受講を完了するには1ヶ月かかる見込みです。

企業のセキュリティレベル向上には、従業員のセキュリティ教育が不可欠です。

日頃から繰り返しセキュリティ教育を実施し、従業員のセキュリティ意識・モラルを定着させましょう。

D4 開封した不審メールを調査 100 pt

セキュリティベンダより「添付ファイルは、最近流行っているマルウェアの亜種であることが判明。対応したアンチウイルスソフトの定義ファイルを緊急アップデートしました。」と回答がありました。

社内のセキュリティ担当では判断がつかない場合は、セキュリティベンダへ支援を依頼しましょう。

事前にセキュリティベンダの問合せ先を把握しておくことも重要です。

D9 全従業員へ注意喚起 100 pt

他の不審メール受信者が不審メールを開封することを防止できました。

不審メールの特徴（送信元アドレスやメールの内容など）や受信した時の対処方法、問合せ先を併せて周知しましょう。

D8 他従業員の不審メール受信状況を確認 100 pt

同様の不審メールを受信した従業員が10人見つかり、開封しないよう指示しました。
また、メールサーバで不審メールの送信元アドレスを受信拒否するよう設定しました。

特定企業を狙った不審メールでは、複数の従業員に対して同様のメールが届く場合があります。

同様の不審メールが届いていないか確認し、受信者にはメールを開封しないよう注意喚起しましょう。

D7 PC1の利用者へヒアリング 100 pt

添付ファイル開封後、端末の動作が重くなったことがわかりました。

マルウェアに感染した疑いのある端末でどのような操作をしたのか、端末の挙動に変化がないか等を確認することは、初動調査における重要なポイントです。

D10 CISOへ報告 2h

「外部セキュリティ機関より当社から不審な通信が発生しているとの連絡を受け、調査を開始したこと」をCISOへ報告します。

D11 外部セキュリティ組織へ相談 2h

外部セキュリティ機関(JPCERT/CCなど)へ相談します。

D12 セキュリティ情報を収集 2h

インターネットから、当社に類似した事象や対策方法等の情報を収集します。

D13 サイバー保険に加入 3h

サイバー保険に加入します。

D14 データ暗号化 3h

PCやサーバのデータを暗号化するよう情報システム部門に依頼します。

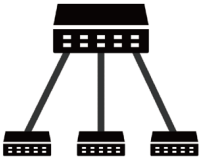
D15 WAF(Web Application Firewall)を導入 3h

WAFを導入し、通販サイトへの不正アクセスをブロックするようWEBセキュリティ担当に依頼します。

D16 外部との通信ログ調査(Firewall、Proxy) 3h

FirewallやProxyに不審な通信を示すログがないか調査をするよう、SOCに依頼します。

D17 社内のネットワークセグメントを分割 3h



部署ごとにネットワークセグメントを分割するよう情報システム部門へ依頼します。

D18 CISOへ報告 3h

不審な通信の発生元端末が顧客情報データベースにアクセスしていたこと、および被害想定や今後の対応方針を報告します。

D12 セキュリティ情報を収集 60 pt

当社と同じ不審通信元を含む注意喚起情報が公開されていたため、Firewallでブロックするよう設定しました。

JPCERT/CCやIPAのホームページでは、最新のセキュリティ脅威情報や対策方法を公開しています。

日頃から最新情報をチェックしましょう。

D11 外部セキュリティ組織へ相談 100 pt

類似事例や初動対応方法を教えてもらえました。

JPCERT/CCなどの外部セキュリティ組織に相談すると、類似事例情報やインシデント対応方法などの支援を受けることができます。

D10 CISOへ報告 20 pt

CISOからインシデントの重大性を判断した上で、再度報告するよう求められました。

CISOへ報告する際は、被害状況や顧客・取引先等への影響、また今後の対応方針も含めて報告しましょう。

あらかじめ、報告基準を定めておくことが重要です。

D15 WAF(Web Application Firewall)を導入 0 pt

WEBセキュリティ担当より、「WAFの導入には１ヶ月必要」との回答がありました。

WEBサイトへのサイバー攻撃（今回は発生していない）に対して有効な対策ですが、導入には時間がかかります。

計画的に導入を進めましょう。

D14 データ暗号化 0 pt

情報システム部門より、「データ暗号化には１ヶ月必要」との回答がありました。

データ暗号化は、万が一攻撃者が秘密情報などを取得しても閲覧されることを防ぐことができるため、情報漏洩には有効な対策ですが、導入には時間がかかります。

計画的に導入を進めましょう。

D13 サイバー保険に加入 0 pt

保険会社より見積りを入手しましたが、今回のインシデントは補償されないと回答がありました。

サイバー保険に加入すると、インシデント発生時に契約範囲内で補償金を受け取ることができます。

補償内容は保険により様々ですが、例えばサイバー攻撃の調査費用などの補償を受けられることがあります。

D18 CISOへ報告 100 pt

今後の対応方針が了承され、対応体制が強化されました。

被害状況を特定（または最大の被害を想定）し、今後の対応方針も含めた報告を実施しましょう。

あらかじめ、報告基準を定めておくことが重要です。

D17 社内のネットワークセグメントを分割 0 pt

情報システム部門より、「ネットワークセグメントの分割は、すぐにはできない」との回答がありました。

ネットワークセグメントを分割することにより、マルウェア感染時の拡大防止だけでなく、情報へのアクセス制限強化を図ることもできます。

ネットワークセグメントの分割による業務への影響を考慮し、計画的に実施しましょう。

D16 外部との通信ログ調査（Firewall、Proxy） 100 pt

C＆Cサーバと不審な通信をしているPC2を特定しました。
（しかし、暗号化通信されていたため内容は不明。）
C＆Cサーバとの通信をブロックするよう設定を追加しました。

インシデント発生時、ログ調査ができるようあからじめ適切なログ設定をしておきましょう。

D19 外部セキュリティ組織へ相談 2h

外部セキュリティ機関(JPCERT/CCなど)へ相談します。

D20 セキュリティ情報を収集 1h

インターネットから、当社に類似した事象や対策方法等の情報を収集します。

D21 Active Directoryサーバーのログ調査 3h

不正な権限昇格等が行われていないか、ActiveDirectoryの管理者にログ調査を依頼します。

D22 通販サイト停止を指示 4h

顧客情報が漏洩したことを想定し、通販サイトの停止をシステム担当に依頼します。

D23 PC2をフォレンジック調査 3h

PC2のフォレンジック調査をセキュリティベンダへ依頼します。

D24 データ暗号化 3h

PCやサーバのデータを暗号化するよう情報システム部門に依頼します。

D25 顧客情報データベースのアクセス権限見直し 3h

不要なアカウントの無効化、権限見直し、パスワードのリセットをシステム担当に依頼します。

D26 顧客情報データベースのログ調査 3h

顧客情報データベースでどのような操作が行われたのか、詳細調査をシステム担当に依頼します。

D27 インシデント対応規則・手順の策定 4h

インシデント対応規則、対応手順の策定チームを発足します。

D21 Active Directory サーバーのログ調査 80 pt

不正な権限昇格が行われた形跡は見つかりませんでした。

攻撃者は、マルウェア感染した端末や端末利用者のアカウントを悪用して、Active Directoryドメインや各種システムの管理者権限を奪取しようと試みる場合があります。

D20 セキュリティ情報を収集 20 pt

当社で発生中のインシデント対応に有効な情報は得られませんでした。

IPAやJPCERT/CCのホームページでは、最新のセキュリティ脅威情報や対策方法を公開しています。

日頃から最新情報をチェックしましょう。

D19 外部セキュリティ組織へ相談 100 pt

類似事例や初動対応方法を教えてもらえました。

JPCERT/CCなどの外部セキュリティ組織に相談すると、類似事例情報やインシデント対応方法などの支援を受けることができます。

D24 データ暗号化 0 pt

情報システム部門より、「データ暗号化には１ヶ月必要」との回答がありました。

データ暗号化は、万が一攻撃者が秘密情報などを取得しても、閲覧されることを防ぐことができるため情報漏洩には有効な対策ですが、導入には時間がかかります。

計画的に導入を進めましょう。

D23 PC2をフォレンジック調査 80 pt

セキュリティベンダより、「深夜時間帯に、不審な暗号化ファイルが削除された形跡を発見した。しかし、ファイルは復元できなかった」と連絡がありました。

フォレンジック調査することで、具体的な攻撃手法や被害状況、影響範囲を把握できることがあります。

D22 通販サイト停止を指示 0 pt

予告なく通販サイトを停止したため、顧客から苦情の問合せが殺到しました。
また、社内の関係部署から状況説明を要求されました。

業務停止（通販サイト停止）が必要な場合には、必ずCISOへ報告し、判断を仰ぎましょう。

業務停止後に影響が生じる関連部署との連携した対応が必要です。

D27 インシデント対応規則・手順の策定 0 pt

検討チームを発足し、活動を開始しました。
インシデント対応規則、対応手順は、1ヶ月後に完成する予定です。

インシデント対応を混乱なく適切に実施するためには、インシデント対応規則や対応手順が不可欠です。

さらに、日頃よりインシデント対応訓練を実施し、有効性の確認や問題点の改善を繰り返しましょう。

D26 顧客情報データベースのログ調査 100 pt

使われていないはずの管理者アカウントを利用し、顧客情報（氏名、性別、年齢、住所を含む）１０万件にアクセスしていることがわかりました。

不正な操作が発生した際、直ちに検知できるよう日頃からログの監視を行いましょう。

想定外の操作が発生した際には、アラート通知することが有効です。

D25 顧客情報データベースのアクセス権限見直し 100 pt

業務に必要最低限のアクセス権限に見直すことができました。

アクセス権限を正しく管理することで、不正アクセスを防止することができます。

D28 データ暗号化 3h

PCやサーバのデータを暗号化するよう情報システム部門に依頼します。

D29 WAF(Web Application Firewall)を導入 3h

WAFを導入し、通販サイトへの不正アクセスをブロックするようWEBセキュリティ担当に依頼します。

D30 サイバー保険に加入 3h

サイバー保険に加入します。

D31 法務部門に今後の対応を相談 2h

今後発生が予想される法務的な対応を依頼します。

D32 カスタマーサポート部に今後の対応を相談 2h

今後発生が予想されるお客様向け対応を依頼します。

D33 広報部に今後の対応を相談 2h

プレスリリースや記者会見に向けた対応を依頼します。

D34 従業員へ情報漏洩発生について伝達 2h

情報漏洩の発生、及び、従業員が取るべき行動について伝達します。

D35 外部関係機関へ情報漏洩を報告 2h

個人情報保護委員会に情報漏洩が発生したことを報告します。

また、警察に不正アクセス事件として相談・通報します。

D30 サイバー保険に加入 0 pt

保険会社より見積りを入手しましたが、今回のインシデントは補償されないと回答がありました。

サイバー保険に加入すると、インシデント発生時に契約範囲内で補償金を受け取ることができます。

補償内容は保険により様々ですが、例えばサイバー攻撃の調査費用などの補償を受けられることがあります。

D29 WAF(Web Application Firewall)を導入 0 pt

WEBセキュリティ担当より、「WAFの導入には１ヶ月必要」との回答がありました。

WEBサイトへのサイバー攻撃（今回は発生していない）に対して有効な対策ですが、導入には時間がかかります。

計画的に導入を進めましょう。

D28 データ暗号化 0 pt

情報システム部門より、「データ暗号化には１ヶ月必要」との回答がありました。

データ暗号化は、万が一攻撃者が秘密情報などを取得しても、閲覧されることを防ぐことができるため情報漏洩には有効な対策ですが、導入には時間がかかります。

計画的に導入を進めましょう。

D33 広報部に今後の対応を相談 100 pt

プレスリリースや記者会見に必要なドキュメントや想定Q＆Aが作成されました。

プレスリリースの内容によっては、事業への影響がさらに拡大する可能性があります。発表内容や想定Q＆Aが、誤解を生じさせない明確な内容であるか、確認しましょう。

また、お客様目線に立った内容となっているか確認することも重要です。

D32 カスタマーサポート部に今後の対応を相談 100 pt

お客様へ案内する内容や方法の検討、問合せ窓口体制が強化されました。

お客様に生じる影響や実施頂くべき対応（パスワード変更）等を正確に伝えましょう。

また、対応方法が不明な場合には、速やかにエスカレーションするよう依頼しましょう。

D31 法務部門に今後の対応を相談 100 pt

過去に発生した他社のインシデント対応事例の情報収集、顧客や取引先に影響が発生した場合の損害賠償等について検討が開始されました。

顧客や取引先、関係省庁等に向けた幅広い対応が必要となります。

対外的な発表前（プレスリリースや記者会見）に相談しましょう。

D35 外部関係機関へ情報漏洩を報告 100 pt

情報漏洩について現時点で把握している内容を報告し、今後必要となる対応を相談します。

個人情報漏洩が発生した際は、速やかに個人情報保護委員会へ報告する必要があります。

また、警察に不正アクセス事件として相談・通報する事で、対外的にきちんとした対応をしている事を示せます。

D34 従業員へ情報漏洩発生について伝達 80 pt

従業員が当社で情報漏洩が発生したことを認識し、今後とるべき行動が周知されました。

全従業員向けに伝達する内容は、プレスリリース予定の内容と同じ内容に留めましょう。

また、外部からの問合せに対して、個人の判断で対応しないよう、対応方法についても併せて周知しましょう。

月曜日
状況カード

火曜日
状況カード

水曜日
状況カード

木曜日
状況カード

残業！
残業カード

E3 顧客情報データベースへのアクセス

水曜日

SOCが調査した結果、不審な通信の発生元端末（PC2）が特定され、通販サイトの顧客情報データベースにアクセスしていたことが分かりました。

E2 不審な通信の連絡

火曜日

PC１を調査した結果、最近流行っているマルウェアの亜種に感染していたことが判明しました。アンチウイルスソフトのパターンファイルが更新され、対応が完了しました。

外部セキュリティ機関より当社から不審な通信が発生していると連絡がありました。

E1 不審メールを開けてしまいました!

月曜日

PC1の利用者から「不審なメールの添付ファイルを開封してしまった!」と連絡がありました。

Z1 残業（＋６時間）を指示

残業！

利用できる工数を６時間追加できます。

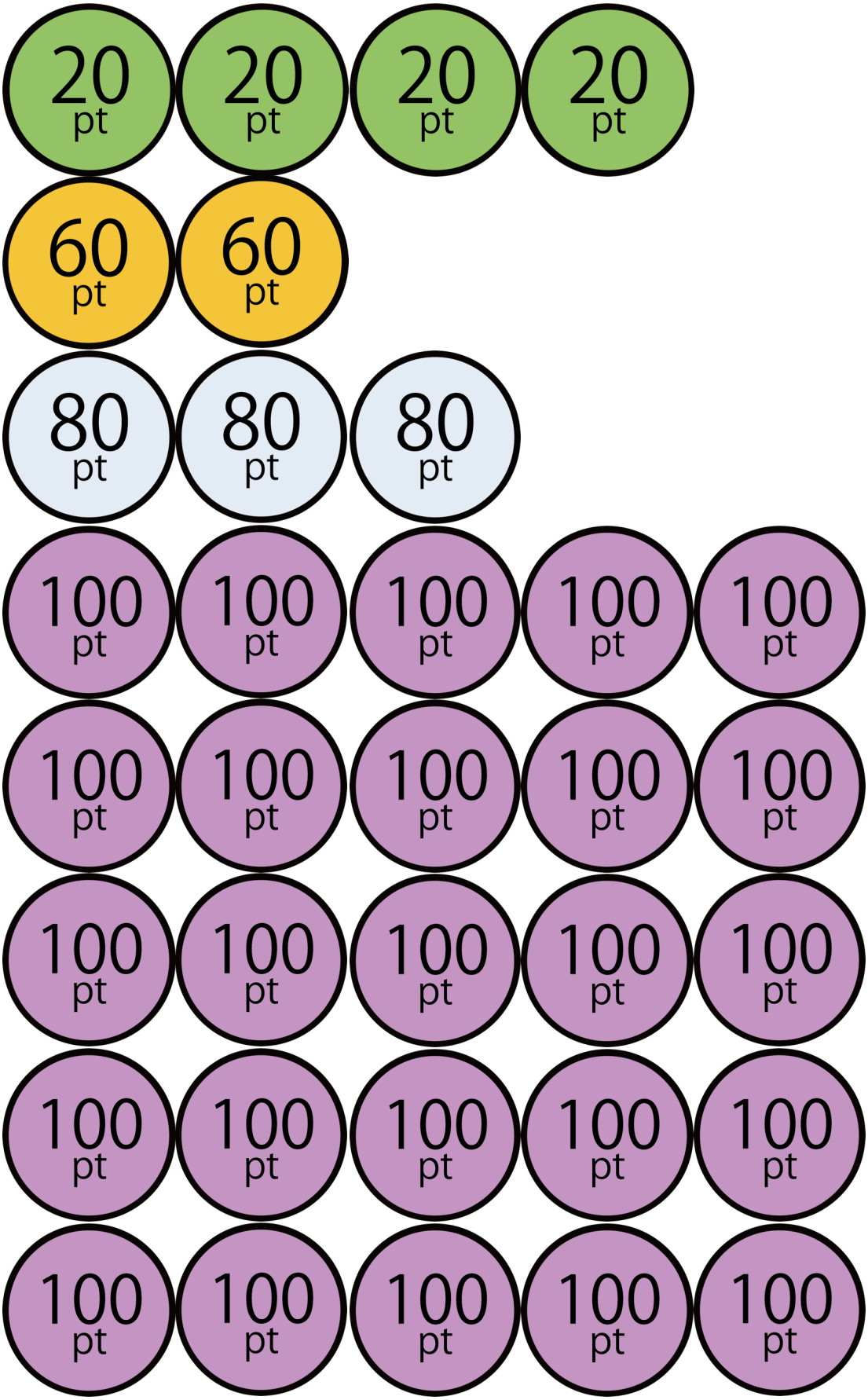
（ゲーム中、1回のみ利用可能）

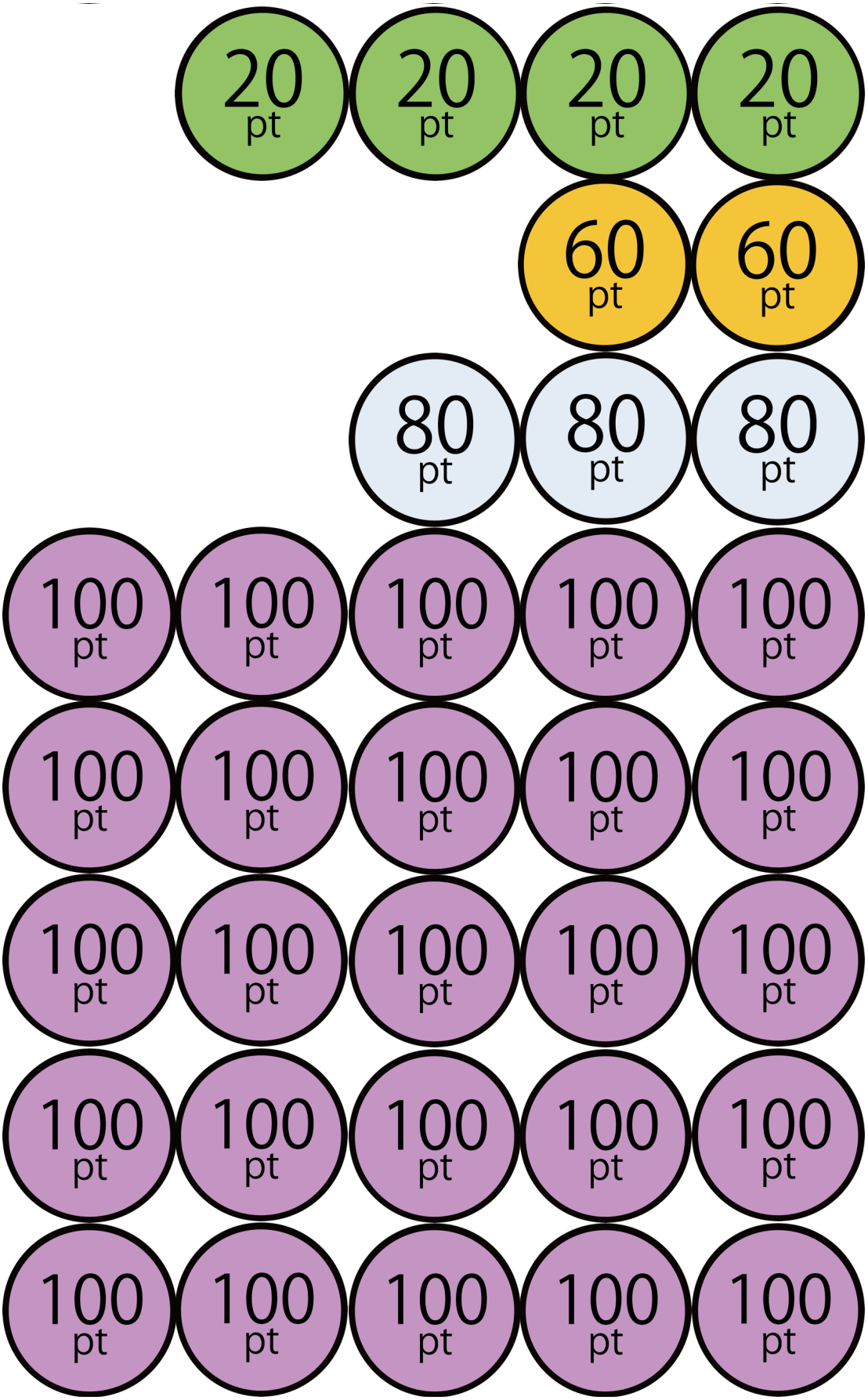
E4 顧客情報漏洩が発覚

木曜日

顧客情報データベースとPC2を調査した結果、10万件の個人情報が不正に取得され、社外に送信されていることが判明しました。

外部機関より当社の顧客情報が漏洩していると連絡がありました。


20 pt
20 pt
20 pt
20 pt
60 pt
60 pt
80 pt
80 pt
80 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt
100 pt


20 pt
20 pt
20 pt
20 pt
60 pt
60 pt
80 pt
80 pt
80 pt
100 pt