1．顧客メールアドレス漏えい対策（Enterprise Protection）の利用例

～標的型メール攻撃の被害拡大を防ぐ～

Safety Answer はインターネットへ公開されているメールアドレスへ届いたメールを、社内ネットのメールアドレスへ転送します。社内ネットのメールアドレスへ届く外部からのメールは、送信者アドレスが匿名化されて届きます。顧客メールアドレス漏えい対策

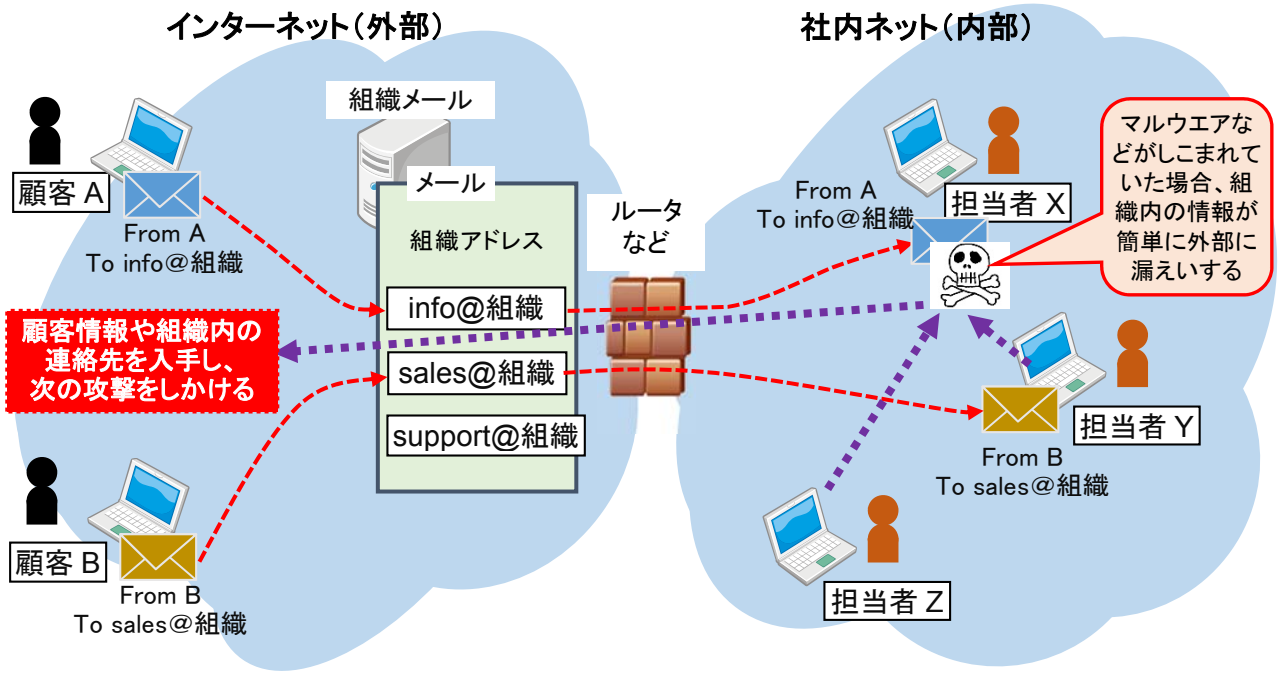
送信者のアドレスが匿名化されたメールを受信した利用者は、匿名化されたアドレス宛にメールを送信することで、**Safety Answer** によってメールの宛先が元々のメール送信者のメールアドレスに戻され、正確にメールの送信者へメールが送信されます。

外部から届くメールの送信者アドレスを匿名化することで、社内ネットで外部からのメールを受信する利用者は、メール送信者の実際のメールアドレスを知らずにメールを受け取り、メールを返信することができます。さらに、このメール送信者の匿名化されたアドレスは、メールの受信者個人のアドレス専用に割り当てられたメールアドレスであって、メールの送信者へ返信ができるのは、メールを受信した本人に限定されます。

① 一般的なメール利用形態

組織で運用するメールアドレスを使って、直接担当者が自身の PC でメールを受信・送信します。担当者の PC には、顧客のメールアドレスが蓄積され、常時情報漏えいの危険にさらされています。

標的型攻撃の対象となりマルウエアなどが侵入した場合、自身の PC に蓄積されている顧客のメールアドレスのほか、組織内の PC のメールアドレスも漏えいし、二次、三次の攻撃の対象となります。



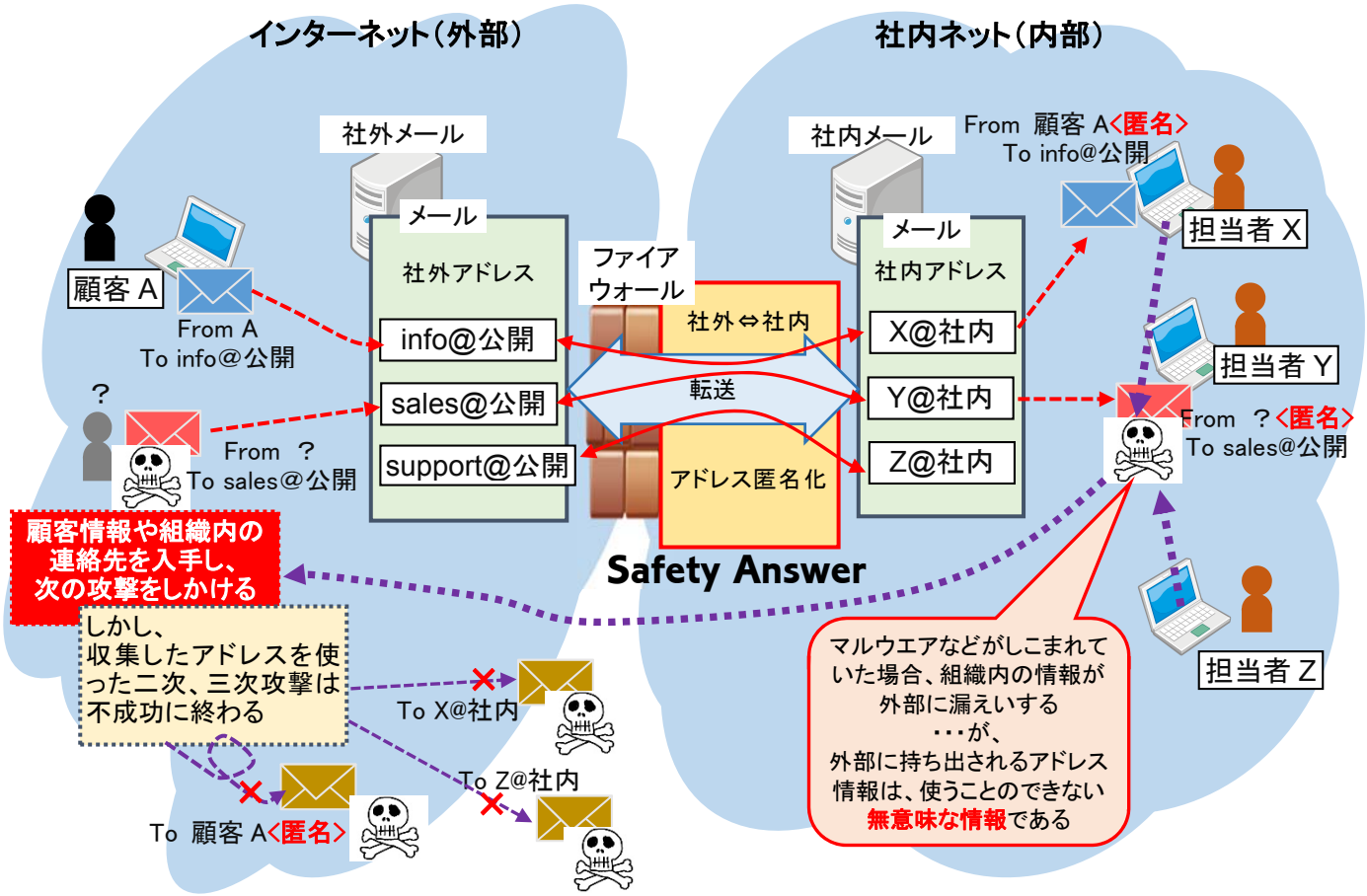
※ 組織メールサーバは、ISP のクラウドサーバなどを利用した例

② 社内と社外をメールアドレスで分離

ファイヤーウォールの内部に、社内ネットだけで利用できるドメインを使用したメールシステムを運用します。

外部から届くメールは、**Safety Answer** が内部ドメインの担当者へ転送すると同時に、送信者のアドレスを匿名化してメールを届けます。

担当者が顧客へメールを送信する場合は、自分専用に匿名化された顧客のアドレスへメールを送信することで、**Safety Answer** が正確に顧客の本当のメールアドレスへメールを送信します。



たとえ社内の PC がマルウエアに感染し、顧客のメールアドレスや社内のメールアドレスが外部へ漏えいしたとしても心配はありません。

Safety Answer によってアドレスが匿名化されている顧客へはメール送ることはできません。

また、社内の利用者に対しても、外部から直接メールを送信することができません。

これにより、**メールを使った二次、三次の侵入を防ぐ**ことができ、標的型メール攻撃の被害拡大を止める効果を発揮します。